Advance Counter Terrorism for Lebanon Security

Title of the assignment

Case-study training on sectorial cyber risk assessment

1 - General context and objectives

A continuous dialogue between the European Union and Lebanon has been focussing, for several years, on security and counter-terrorism. Aligned with the European Neighbourhood Policy and the European Union Global Strategy on Foreign and Security Policy, an agreed roadmap addresses the areas of counter-terrorism, justice and law enforcement, countering terrorism financing and violent extremism, among others.

The **project** "Advance Counter Terrorism for Lebanon security" (2020-2023), led by the International and Ibero-American Foundation for Administration and Public Policy (FIIAPP), aims at reinforcing national capacities in Lebanon to react to the threats of terrorism and organized crime while promoting rule of law and human rights, in line with international standards.

Three specific objectives are pursued:

SO 1: To strengthen the regulatory framework and national response against terrorism in line with international standards. This includes supporting counter-terrorism interagency coordination.

SO 2: To enhance protection and response against terrorism through an improved cybersecurity national system.

SO 3: To apply a rights based approach to CT/VE cases by law enforcement officials and Courts. This includes strengthening a lawful collection of evidences to be legally used before the Court.

The digitalisation of society translates the challenges of terrorism and organized crime into the cyberspace. Therefore, the project counts as its **specific objective 2** to enhance protection and response against terrorism and crime through an improved cybersecurity national system.

In close relation with the Lebanese National Coordination for the project, key **stakeholders** include officials from the Lebanese Law Enforcement Agencies, such as the Lebanese Armed Forces (LAF), the Internal Security Forces (ISF), the General Security (GS) and the State Security (SS) as well as civil servants of various ministries and public authorities in charge of supervising critical infrastructure operators, in sectors such as Defence, Interior, Telecommunications, Banking, Health and so forth. Besides, Parliamentary Committees, representatives of the National Human Rights Commission and members of Civil Society Organizations will count amongst regular counterparts as well. Finally, partnerships with private companies and Universities will be highly promoted.

Two **results** are expected in the domain of cybersecurity: the enhancement of national capacity to prevent and counter cyber-terrorism and cyber-organized crime, on the one hand, and the enhancement of a general awareness on cybersecurity and cybercrime, on the other hand.

Respond to and counter terrorism and crime

A legitimate cyber policy prerogative for the Lebanese government is the field of development and resilience, aimed at building functioning and accountable institutions essential for effectively responding to and recovering from cyber-attacks, while ensuring compliance with human rights and the rule of law.

The efforts to be made in terms of incident response have two aspects, the second of which depends on the first:

- Adopt risk management and crisis management procedures,
- Training to enhance mitigation and remediation at the national level.

Then, other efforts are to be made in terms of response, that concern the judicial aspect, meaning the training of investigation units for the purpose of prosecution.

2 - Description of the assignment

Background

Lebanon adopted a national cybersecurity strategy in 2019. This strategy promotes the use of a state-of-the-art methodology to assess cyber risks within critical operators. Initial efforts have been made in this direction, particularly at the academic level.

A training activity was deployed in May 2021 for the benefit of members of various public critical entities. The participants were trained on a state-of-the-art scenario-based cyber risk-assessment methodology called Ebios Risk Manager. They shall now embark on a study case cyber risk assessment.

Objective

The purpose of this activity is to support the teams engaged in cyber risk analysis, drawing on the skills recently acquired, by coaching them as they pursue their case studies and accompanying them to the conclusion and defend of their studies before their managers.

Expected result

Lebanese critical operators' capacities on cyber risk analysis are enhanced by completing pilot study cases for the benefit of their organizations.

3 - Course of the assignment

Tasks required

- Study the context of implementation of this project
- Meeting with the Lebanese National Coordinator for the project
- Coaching of the teams trained for the effective use of a state-of-the-art scenario-based cyber risk-assessment methodology, as they implement a case-study
- Coaching of the teams as they conclude their studies and defend them before their managers

Deliverables and outputs of the mission

- Case-study adapted risk-analysis templates
- Activity Report (list of people met / recommendations for improvement / experience feedback – according to the templated provided)

NB: the deliverables are to be drafted in English.

4 - Location, duration and financing of the assignment

Places of the mission

The mission will be deployed in Beirut, Lebanon.

Meetings shall be held in the city as well as outside the city, to be determined accordingly to the stakeholders' facilities.

Nevertheless, depending of Covid-19 restrictions, all or part of the agenda may be carried out remotely.

Period of the mission

The mission will take place in June and July 2021.

Duration of the mission

The estimated duration is 6 working days.

Financial aspects

The expert will receive fees for each working day.

A working day can be invoiced if the expert spends at least seven working hours, excluding any break. STEs are bound by the rules on hours of work in force in the Lebanese administration.

5 - Required expertise

Qualifications and skills

Advance academic degree (Master's level or upper) or equivalent senior experience in cyber risk-assessment.

Excellent pedagogical skills.

Mastery of English.

General professional experience

12 years of experience in the field of cybersecurity and risk-assessment.

Specific professional experience

5 years of experience in scenario-based risk-assessment.