Expertise en «cyber threat intelligence assessment» - Advance Counter Terrorism for Lebanon Security

Terms of Reference

LIMITE DE CANDIDATURE

21 Octobre 2021

DURÉE DE LA MISSION

Court Terme

ZONE GÉOGRAPHIQUE

Pays De La Méditerranée Et Du Golfe

Title of the assignment

Assessment on capacity in network supervision, cyber threat intelligence and cyber incident detection, within critical infrastructure in Lebanon

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.

Prevention and protection against terrorism and crime

Cyber risk prevention is above all an inter-ministerial policy aimed at the protection and resilience of critical infrastructure. So, building prevention capacity at the national level requires the initiation of a continuous endeavour, based on an effective collaboration of the capacities held by the LEAs as well as by the most capable economic sectors (telecom, banking, etc.) and finally relying on the academic skills of the university actors and on the encouraging initiatives of innovative digital companies in Lebanon. This effort designs the following activity axes:

- Ability to observe reality (Surveillance probes and Security Operating Centres), in line with the rule of law and in accordance with considerations of proportionality and respect for citizens privacy,
- Generation of knowledge (Cyber Threat Intelligence), by improving coordination between state agencies dotted with investigative resources,
- Translation of this knowledge into guidelines and regulations: these guidelines could consist in mandatory security rules for critical infrastructure operators as well as they could be designed to be delivered more widely, incentivizing security enhancement within voluntary beneficiaries or towards the general population.

2 - Description of the assignment

Background

Initial milestones have been passed in the development of Security Operations Centres within the law enforcement community as well as within some critical operators, notably in the banking and telecom sectors. Successes are also to be reported about Lebanese private initiatives, providing “SOC as a service” to several critical infrastructure operators in the health sector (major hospitals of Beirut), in the banking sector, in the telecom sector and in partnership with academics.

Objective

During this activity, a cyber expert will draw up an inventory of public, academic and private capabilities in terms of network monitoring, cyber threat intelligence and cyber incident detection.

Expected result

Gain a perspective on how Indicators of Compromission (IoC) are identified, shared and searched for in Lebanese critical infrastructure information systems, in order to adapt specific training to be deployed as a national effort in future activities.

3 - Course of the assignment

Tasks required

- Study of all the necessary documentation (i.e. the Inception report of this action and of the Lebanese National Strategy on Cybersecurity)
- Meeting with Cyber Key Expert and the Lebanese National Coordination for the project
- Visit bilaterally the achieved or under development capacities within Law Enforcement Agencies, Critical infrastructure operators in the banking and telecom sectors, as well as academic and private initiatives.

Deliverables and outputs of the mission

- Inventory of public, academic and private capabilities in terms of network monitoring, cyber threat intelligence and cyber incident detection
- Recommendations regarding the design of a training on the establishment of a Cyber Threat Intelligence Centre
- Recommendations regarding the design of a training in early detection of cyber-attacks and intelligence sharing with critical operators
- 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 November 2021.

Duration of the mission

The estimated duration is 5 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 security.

Mastery of English is a must. Knowledge in other languages in use in Lebanon would be an asset (Arabic or French).

Excellent writing and analytical skill in drafting concept notes and reports.

Very good contact and networking skills.

General professional experience

At least 5 years of professional experience in the field of Cyber Threat Intelligence

Specific professional experience

At least 5 years of professional experience in technology available for cyber malevolence activity early detection.

Experience in 2 capacity building projects in the field of Cyber Threat Intelligence sharing.

Strong knowledge of latest technologies in cyber security is a must.

A comprehensive perspective (auditor-in-training, panellist at workshops, publication of articles) about cyber security challenges would be an asset.