Terms of Reference

Title of the assignment	Mapping the ecosystem of public, academic and private actors, to support the national cybersecurity system
Action	Advance Counter Terrorism for Lebanon Security
Objective	To contribute to improved citizens security against terrorism based on rule of law and human rights.
Specific Objective	SO2 – Improved cyber-security and protection and response against cyber-terrorism.
Output	Op2.1 – Enhanced national capacity on countering cyber-terrorism and cyber-organised crimes.
Activity reference	Op2.1 – 2022 – 2.1.6
Location of the mission	Beirut, Lebanon
Period of the mission	November and December 2022
Number of working days	15
Number of experts	One
Expertise	Non-Key
Profile required	Senior

Advance Counter Terrorism for Lebanon Security

Title of the assignment

Mapping the ecosystem of public, academic and private actors, to support the national cyber security system.

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 Spain´s International and Ibero-American Foundation for Administration and Public Policy (FIIAPP), in consortium with CIVIPOL (France) and Arma di Carabinieri (Italy), 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:

SO1: Improved national response against terrorism, in line with international standards;

SO2: Improved cyber-security and protection and response against cyber-terrorism;

SO3: Improved application of rights-based approach to Counter Terrorism (CT) / Violent Extremism (VE) cases by law enforcement officials and Courts.

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.

Under the general supervision and coordination of the Secretary General of the Council of Ministers and the Higher Defense Council, the project include key **stakeholders** 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.

2 - Description of the assignment

Background

The Lebanon National Cyber Security Strategy was released in June 2019 with the ambition that Lebanon has "*a secure and stable cyberspace, both within the national territory and in international exchanges*". The strategy emphasises that the creation and institutionalization of a National Cyber Security Information System Agency (NCISA) at the national level, is essential to maintain a Lebanese national cybersecurity strategy, to anchor cyber security capacity in a strong legal and regulatory framework, and **to build an ecosystem of public, private and academic actors in Lebanon**.

Two previous activities have been carried out on this "Lebanese cyber and digital ecosystem" topic:

- A.2.2.1: Assessment of Lebanese civil society organizations' (CSO) achievements in terms of cyber-risk awareness-raising;
- A.2.1.3: Development of general partnership protocols and cooperation agreements with public, private and academic actors for the implementation of the National Cyber Security Strategy.

Objective

The purpose of this activity is to build a data mapping of relevant public, academic and private actors in cybersecurity and digital areas, that will be able to support the operations of the future National Cybersecurity Information System Agency (NCISA) and its platforms (CSIRT[1], training centre, awareness-raising platform).

Expected result

An ecosystem of public, private and academic actors, to support the national cyber security system is established and formatted in a database..

3 - Course of the assignment

Tasks required

<u>Analysis of existing documents and meetings with counterparts – 1 working day</u>

- Study the context of implementation of this project;
- Taking note of previous activity reports: 2.2.1 *Assessment of the achievements by Civil Society Organizations (CSO) in terms of cyber-risk awareness-raising* and 2.1.3 *Partnership protocols' design*.
- Meeting with the ACT Project Team.

[1] Cyber Security Incident Response Team.

Ecosystem assessment and mapping – 10 working days

- Develop a taxonomy of key areas of expertise to be addressed in cyber and digital. Key areas of expertise are areas where there is a specific need for supporting the national cyber security system in Lebanon, including operations of the future national cyber security agency and its platforms (CSIRT, training centre, awareness-raising platform). See tentative taxonomy in annex.
- Identify Lebanese and main international actors (public, private and academic), specialized or involved in the key areas of expertise, benefiting from the work accomplished during previous activity 2.2.1 on *assessment of the achievements by Civil Society Organizations (CSO) in terms of cyber-risk awareness-raising*.
- Develop a questionnaire to assess areas of expertise for each voluntary actor, benefiting from the work accomplished during previous activity 2.2.1.
- Mapping local Lebanese expertise as well as main international actors on the basis of feedback from questionnaires. This mapping will serve as a basis for developing future tenders and framework contracts for outsourced services between the Lebanese government and the public, private, academic actors of the ecosystem.
- Identify areas of expertise that are not or are poorly covered by local Lebanese actors.

Developing a basic database – 4 working days

- Group all the collected information in an organized repertoire (small data base) with an updating tool facilitating the consultation based on the needs. This shall be based on the questionnaire fields to be part of the deliverables.

The ecosystem mapping shall be aligned with the mandate, missions and support needs of the future NCISA, as defined in activity 2.1.4 "*Assessment on the legal bases requirements for the establishment of the National Cyber Security Information System Agency and development of the action plan*".

Deliverables and outputs of the mission

1. Cyber and digital ecosystem mapping (document):
    - Taxonomy of key areas of expertise to support the NCISA's mandate and missions,
    - Ecosystem mapping of Lebanese and international actors,
    - Areas of expertise not or poorly covered by local Lebanese actors,
    - Recommendations,
    - Annexes (e.g. assessment questionnaires).
2. Electronic tool for collected data (basic data base or dynamic catalogue).
3. Activity report

The deliverables of the activity will then constitute an input for the NCISA to establish partnership program and protocols, through calls of tenders.

NB: the deliverables are to be drafted or translated in English.

4 - Location, duration and financing of the assignment

Places of the mission

The mission will take place in Beirut, Lebanon.

The meetings and workshops shall be held in the city as well as outside the city, to be determined accordingly to the stakeholders' facilities.

Period of the mission

The mission will take place in November and December 2022.

Duration of the mission

The estimated duration is 15 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 – Senior expert

Qualifications and skills

Advance academic degree (Master's level or upper) or equivalent senior experience in digital or IT.

Mastery of English and Arabic is a must. Mastery of French would be an asset.

General professional experience

At least 12 years of professional experience in the fields of cyber security and data privacy.

Specific professional experience

At least 5 years of professional experience in assessing and mapping business ecosystems in the fields of cyber security, digital and IT. Knowing Lebanese cyber and IT ecosystem would be an asset.

At least one experience in developing databases.

At least one experience in implementing partnerships protocols or public-private programs in Lebanon.

6 – Annex – Tentative taxonomy of key areas of expertise in cyber and digital

Technical areas
Cyber security: securing or strengthening ICT systems and networks[2]
Cyber risk assessment (e.g. EBIOS, risk treatment plans…)
Cyber crisis management, digital resilience[3]
Crisis communication
Security audits / pentesting
Cyber threat intelligence
Security accreditation of ICT systems and networks
Cyber and digital regulatory framework (e.g. legal assessment)
Cyber defense (e.g. event monitoring, early detection, incident response, IoC…)
Digital forensics investigation (e.g. dark web, crypto currencies, e-evidence…)
Data privacy
Areas of service provision
Expertise – Consulting (including compliance)
Development of security products or services
Evaluation, certification, qualification of security products, services or providers
Development of digital platforms and software
Training (academic training courses, training exercises / simulations)
Education – Awareness raising
SOC – SIEM – CSIRT services
Research & Development in specific cyber or digital areas (e.g. artificial intelligence)

IoC: Indicator of Compromise.
SOC: Security Operations Centre.
SIEM: Security information and event management.
CSIRT: Cyber Security Incident Response Team.

[2] E.g. Authentication and access control, Computer administration management, Encryption and PKI management, Security of interconnections, Patch management…

[3] E.g. Standard Operating Procedures for managing cyber incidents, Business Continuity Plan…