



The Project is funded
by the European Union



Advance Counter Terrorism for Lebanon Security

Terms of Reference

Title of the assignment

Workshop on the endorsement of initiatives aimed at mobilizing various public, private and academic actors in the first steps towards the implementation of the National Cyber Security Strategy.

1 - General context and objectives

A continuous dialogue between the European Union and Lebanon has been focused, 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 evidence 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, through its **specific objective 2**, will enhance protection and response against terrorism and crime through an improved cybersecurity national system.

The project will work in close relation with the Prime Minister National Coordination Unit for Cybersecurity, and with key **stakeholders** such as the Lebanese Armed Forces (LAF), the Internal Security Forces (ISF), the General Security (GS) and the State Security (SS) as well as with civil servants from various ministries and public authorities in charge of supervising critical



The Project is funded
by the European Union



Advance Counter Terrorism for Lebanon Security

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 also participate. Finally, partnerships with private companies and Universities will be highly promoted.

Two **results** are expected in the domain of cybersecurity. On the one hand, the national capacity to prevent and counter cyber-terrorism and cyber-organized crime is enhanced; and on the other, the general awareness on cybersecurity and cybercrime is improved.

This project contributes to the rights-base implementation of the Lebanese national cybersecurity strategy adopted in 2019, notably the promotion of an inter-departmental and coordinated national cybersecurity effort.

Cyber risk prevention is, above all, an inter-ministerial policy aimed at the protection of critical infrastructure. So, building prevention capacity at the national level requires the initiation of a continuous endeavour in identifying attackers' modus operandi, sharing cyber threat intelligence and designing and implementing security requirements, specifically to the protection of critical operators. This implies enhancing an effective collaboration of the capacities held by the Law Enforcement Agencies and by the most capable economic sectors (telecom, banking, etc.) as well as relying on the academic skills of the university sector and supporting initiatives of innovative digital companies in Lebanon.

In terms of response, a legitimate cyber policy prerogative of the Lebanese government is the field of development and resilience, aimed at building functional and accountable institutions to effectively manage crisis and recover from cyber-attacks, a capacity raised from a cyber risk assessment and management.

Finally, raising awareness requires training the Lebanese society in technical measures to protect from cyber threats in the daily use of digital technology, and raising awareness on the importance of personal data protection, as well as dealing with the current issue of freedom of expression and access to information in a digital world where sensationalism, false news and manipulation of information operate.

2 - Description of the assignment

Background

Terrorism and organised-crime are an area of concern for everyone in Lebanon. Therefore, all stakeholders (Law Enforcement Agencies, Civil Society Organisations, Industry, Universities, lawyers, journalists, etc.) are required for raising awareness and promoting the adoption of preventing policies



The Project is funded
by the European Union



Advance Counter Terrorism for Lebanon Security

Partnerships involving public and private actors, civil society organisations and universities will help in the definition and deployment of a balanced preventive policy at large scale, that will promote the development of national capacities as well as mobilize the vigilance of the Lebanese society.

Objective

This activity will provide **methodological and legal support** for the **drafting of protocols** aimed at officially **endorsing partnership initiatives** that shall be fostered in order to mobilize public, academic, civil society and other private actors for the launching of collective efforts in terms of capacity building and awareness-raising in the cyber security domain.

These partnership initiatives are indeed intended to stimulate the technical efforts of the critical operators to implement cybersecurity prevention policies as well as to deploy cyber risk general awareness programs.

During this activity, the selected short-term expert, acting as a policy expert, will accompany the beneficiary partners by sharing best practices and supporting them in the drafting of protocols.

Expected result

An administrative framework has been set up that allows the **establishment of partnership protocols** involving public and private operators, civil society and academics.

3 - Course of the assignment

Tasks required

- Study of all the necessary documentation (i.e. the Inception report of this action and the Lebanese National Strategy on Cybersecurity)
- Census and analysis of existing memorandum of understanding between the stakeholders involved – some already exist, for example between Law Enforcement Agencies and Universities
- Analysis of the usage of these MoU, based on available return of experience and completed with interviews
- Conception of a legal and administrative framework aimed at structuring public, academic, civil society and other private actor partnership protocol
- Preparation and conduct of a proof of concept collective Workshop
- Drafting conclusions and report



The Project is funded
by the European Union



Advance Counter Terrorism for Lebanon Security

Deliverables and outputs of the mission

- Analysis of existing memorandum of understanding established between beneficiary partners, for example between Law Enforcement Agencies and Universities, or between Universities and Private companies.
- Conceptual paper which includes recommendations for drafting partnership protocols between public, academic, civil society and other private actors, answering Lebanese legal requirements
- Proof of concept collective workshop facilitation content
- Standard partnership protocol, easy to adapt to the circumstances of different beneficiary partners and other stakeholders.
- Activity Report (list of people met / recommendations for improvement / feedback).

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

Period of the mission

The mission will be held in December 2020 or in January 2021.

Duration of the mission

The duration of the mission is estimated in 8 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.



The Project is funded
by the European Union



FIIAPP
COOPERACIÓN ESPAÑOLA



Advance Counter Terrorism for Lebanon Security

5 - Required expertise

Qualifications and skills

Advance academic degree in public management or senior experience in public management.

Mastery of the European languages in use in Lebanon: English and French. Fluency in Arabic would be an asset.

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

Very good social and networking skills.

General professional experience

At least 12 years of professional experience in the field of public management.

Wide experience in designing administrative rights-based and legal documents.

Specific professional experience

An in-depth knowledge (at least 3 years) of the Lebanese legal and administrative procedures in usage for partnership elaboration is required for this mission.

A significant professional experience (at least 2 years) on the implementation of public-private programs, connected with academics and civil society would be a strong asset.

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