2.1.12 : Digital forensic investigation – Darkweb

LIMITE DE CANDIDATURE

21 Janvier 2022

DURÉE DE LA MISSION

Short Term

ZONE GÉOGRAPHIQUE

Pays De La Méditerranée Et Du Golfe

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.

Description of the assignment

Background

The Dark Web contains numerous marketplaces where criminals can sell and buy illegal products, such as databases stolen during computer attacks, components and tutorials for the development of explosives or all kinds of illegal trafficking (arms, drugs, etc.).

Terrorists and organized criminals use this area to opacify their activities and therefore, detecting suspicious activity of organised crime or preparation of terrorist acts has become a necessary function of law enforcement.

Objective

To increase the capacities of law enforcement agents and officers to detect suspicious activity of organised crime or preparation of terrorist acts, focussing on the capacity to use state-of-the-art methods and tools of investigation on the Dark Web.

Expected result

The forensics laboratories and investigation units of the law enforcement agencies are able to investigate on the Dark Web.

3 - Course of the assignment

Tasks required

Conduction of a training offering general knowledge and practical study cases on digital investigation on the Dark Web:

- Presentation of TOR Network, how to browse the Dark Web using appropriate search modalities;
- Case studies: discovering marketplaces, searching for exploits for sale, databases stolen during cyber-attacks, credit cards, etc.;
- Use of specific Deep Web and Dark Web indexing tools (onion links TOR), development of scavenging scripts, etc.;
- How to engage into Chatrooms and use Avatars.

Deliverables and outputs of the mission

- Training curriculum
- Activity Report (list of participants / Agenda / 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.

The training 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 January 2022.

Duration of the mission

The estimated duration is 10 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 cyber forensics investigation.

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

Very good pedagogical skills.

General professional experience

At least 10 years of professional experience in the field of Cyber Security.

Specific professional experience

At least 5 years of professional experience in the field of Cyber Forensics

Experience in Cyber training

Illustrated knowledge on Dark Web

Junior expert

Qualifications and skills

Advance academic degree (Master's level or upper) or confirmed experience in cyber forensics investigation.

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

Very good pedagogical skills.

General professional experience

At least 5 years of professional experience in the field of Cyber Security.

Specific professional experience

At least 3 years of professional experience in the field of Cyber Forensics

Experience in Cyber training

Illustrated knowledge on Dark Web

