

<b>Position Name:</b> Strategic Adviser on Hybrid threats and/or Cyber Security	<b>Employment Regime:</b> Seconded	
<b>Ref. Number:</b> MOL 12*, MOL 13*, MOL 14* ( 3 posts )	<b>Location:</b> Chisinau**	<b>Availability:</b> 24 May 2023
<b>Component/Department/Unit:</b> Operations Department/ Hybrid threats and Cyber security Component	<b>Security Clearance Level:</b> EU SECRET	<b>Open to Contributing Third States:</b> No

### 1. Reporting Line:

The Strategic Adviser on Hybrid threats and/or Cyber Security reports to the Head of Hybrid threats and Cyber Security Component

### 2. Main Tasks and Responsibilities:

- To operationalise the Mission mandate and tasks as set out in the planning documents and the Mission Implementation Plan by advising and mentoring local counterparts on the strategic and operational levels;
- To support the Mission to address areas of structural weaknesses in the performance and accountability of counterparts/institutions and propose relevant solutions;
- To provide strategic advice and assistance to the relevant Moldovan partners in implementing reforms in accordance with the agreed policies and guidelines and in coordination with other international actors and stakeholders;
- To facilitate support and liaison of Member States and like-minded state institutions countering hybrid threats and/or enhancing cyber security;
- According to operational needs, liaison with international bodies and EU institutions, bodies and agencies;
- To identify and advise the relevant Moldovan partners on the capacity and training opportunities on hybrid threats, including foreign information manipulation and interference, and/or cyber security;
- To support the relevant Moldovan partners in identifying the appropriate equipment and infrastructure needed to strengthen resilience to hybrid threats;
- To manage, lead and facilitate projects and interventions on hybrid threats/cyber security;
- To advise, support and facilitate the relevant Moldovan partners in implementing externally funded projects/initiatives in his/her field of expertise;
- To assist in the implementation of training activities on hybrid threats and cyber security;
- To provide analysis and recommendations to the local counterpart in the area of responsibility;
- To liaise closely with other horizontal advisers.

### 3. General Tasks and Responsibilities:

- To contribute to mission reporting in the area of competence;
- To support and contribute to the identification of lessons learnt and best practices in the area of competence;
- To take account of gender equality and human rights aspects in the execution of tasks;
- To perform any other tasks assigned by the Line Manager.

### 4. Essential Qualifications and Experience:

- Successful completion of university studies of at least 3 years attested by a diploma OR a qualification in the National Qualifications Framework which is equivalent to level 6 in the European Qualifications Framework OR a qualification of the second cycle under the framework of qualifications of the European Higher Education Area, e.g. Master's Degree OR equivalent and attested police or/and military education or training or an award of an equivalent rank;  
AND

- A minimum of 5 years of relevant professional experience, after having fulfilled the education requirements.

**5. Essential Knowledge, Skills and Abilities:**

- Good knowledge of hybrid threats and/or cybersecurity, including concrete experience on either strategic or operational levels gained in a governmental agency or equivalent;
- Ability to mentor and motivate local national counterparts;
- Experience of designing and delivering training.

**6. Desirable Qualifications and Experience:**

- Mission experience, e.g., CSDP, UN, OSCE etc.
- Experience in developing strategies, policies and/or operational plans on hybrid threats and/or cybersecurity;
- Experience in coordination and information sharing between governmental agencies and services nationally and internationally;
- For cybersecurity: international recognised certification(s), e.g. ISACA: CISM, CRISC, CISA or ISC2: CISSP, CCSP or similar;
- For cybersecurity: experience on international security standards e.g. NIST Cyber Security Framework, ISO27000 series, CIS Security Controls or similar.

**7. Desirable Knowledge, Skills and Abilities:**

- Knowledge of Russia's hybrid strategies;
- Knowledge of EU policy framework for enhancing resilience to and countering hybrid threats, or for cybersecurity;
- Knowledge of current practices in the field of inter-service cooperation;
- Knowledge of Romanian or/and Russian language.