Position Name: Senior Adviser on Cybersecurity	**Employment Regime:** Seconded	
Ref. Number: ARMP 29	**Location:** Yerevan	**Availability:** ASAP
Component/Department/Unit: Operations / Operational Advice and Capacity Building Unit	**Security Clearance Level:** NOT REQUIRED	**Open to Contributing Third States:** NO

1. Reporting Line:
The Senior Adviser on Cybersecurity reports to the Head of the Operational Advice and Capacity Building Unit.

2. Main Tasks and Responsibilities:

- To operationalise the Mission mandate and tasks as set out in the planning documents and the Mission Implementation Plan (MIP) by advising and mentoring local counterparts on the strategic and operational level as appropriate;
- To provide analysis and recommendations to the local counterpart in the area of responsibility;
- To be embedded within the local institution, when and where relevant, security permitting;
- To ensure timely reporting on activities within the field of responsibility as per planning documents, in particular progress and/or lack of progress;
- To maintain necessary contacts and build relationships with relevant local counterparts;
- To ensure compliance with instruction/direction from Mission management;
- To liaise closely with other Advisers as appropriate;
- To support Armenian authorities in development of national strategies and action plans on countering hybrid threats;
- To advise and support the relevant Armenian counterparts on strengthening their strategic and operational cybersecurity capabilities, as well as their resilience and capacity to respond to malicious cyber activities;
- To advise on the development of cybersecurity legislation and strategies and their implementation;
- To advise on the transformation of the Armenian national cybersecurity framework into the new ecosystem;
- To advice on the introduction of EU standards on NIS2 and on developing public-private partnerships in the cybersecurity domain;
- To advise authorities on understanding the cybersecurity threat landscape;
- To advise on strengthening cyber threat detection and intelligence, situational awareness, information sharing and the establishment of standardised mechanisms to this end;
- To review and provide strategic advice on cybersecurity incident response plans and roadmaps, including those related to DDoS attacks, cloud first policy and Operational Technology (OT) security, as well as on related exercises.
- To support the development of a framework for cyber threat intelligence capabilities;
- To provide advice on the strengthening of Armenian counterparts' capacities for monitoring, analysing and communicating about cybersecurity threats, vulnerabilities and incidents;
- To advise on application of cybersecurity regulation and the choice of suitable cybersecurity equipment and services
- To contribute to the developments of standard operating procedures (SOPs) for the above processes;
- To ensure coherence and cooperation with international partners;
- To ensure Armenian progress is monitored and risk mitigated to ensure attainment of objectives;
- To ensure Armenian counterparts are cognisant of UNSCR 1325 and human rights;
- To identify training and operational support needs, and provide training as relevant.

3. General Tasks and Responsibilities:

- To provide coverage during periods of absence of staff members with other functions as applicable, ensuring continuity of operations and responsibilities;
- To identify and report on lessons learned and best practices within the respective area of responsibility;
- To contribute to and ensure timely reporting on activities within the respective area of responsibility;
- To take into account gender equality and human rights aspects in the execution of tasks;
- To take into account political aspects and exercise discretion, diligence and sound judgement in the execution of tasks;
- To undertake any other related tasks as requested by the Line Manager(s).

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. Bachelor's Degree OR equivalent and attested police and/or military education or training or an award of an equivalent rank;
  AND
- A minimum of 6 years of relevant professional experience, after having fulfilled the education requirements.

5. Essential Knowledge, Skills and Abilities:

- Knowledge of EU cyber policy efforts and processes;
- Knowledge of cybersecurity eco-systems, relevant actors and their interrelations;
- Solid understanding of cyber threats and attacks, including tactics, techniques, and procedures;
- Knowledge of Cyber Governance and compliance activities;
- Excellent analytical and problem-solving skills, with the ability to think strategically;
- Ability to communicate, present and report to relevant stakeholders at both technical and strategic levels.

6. Desirable Qualifications and Experience:

- Experience in working with civilian crisis management policies, relevant EU agencies and international initiatives/policies;
- Knowledge of civilian crisis management at national level;
- Experience in coordination and information sharing between law enforcement and intelligence/security agencies, nationally and internationally;
- Experience in building cyber threat intelligence (CTI) capabilities, including the development of threat intelligence functions and the development of standard operating procedures**;**
- Experience with NIS-2 implementation and public private partnerships;
- Experience in leading relevant programs, such as Cybersecurity Incident Response, CTI or vulnerability management;
- Experience in cooperating across government stakeholders regarding information exchange and utilisation thereof for threat reports;
- Experience in a Cybersecurity Authority, Security Operations Center (SOC) and/or Computer Emergency Response Team (CERT);
- Possession of internationally recognised certifications such as ISACA, CISM, CRISC, CISA or ISC2: CISSP, CCSP or similar.

7. Desirable Knowledge, Skills and Abilities:

- Knowledge of the threat of foreign interference, including cyber threats and attacks, tactics, techniques and procedures;
- Knowledge of Armenian and/or Russian language;
- Knowledge of international legal framework on civilian crises management;
- Knowledge of current practices in the field of interservice cooperation.