END/SNE – JOB DESCRIPTION

Job Framework

Job Title: END/SNE – Security Policy Officer (International Cyberspace Policy and Cybersecurity)

Job Location: EEAS HQ – Brussels

Job Number:

Area of activity: SECPOL Division

Category: AD

Duration of secondment: Two years

Job Content

Overall purpose

Main tasks and responsibilities would be to:

- support the EEAS with expertise in the EU policy making in particular with regard to ongoing international processes and events in cyberspace issues such as the implementation of the EU Cyber Security Strategy, International Security issues in cyberspace, Cyber security dialogues with third countries; facilitating the formulation of common EU positions; support in the EU capacity building and outreach activities etc;
- Contribute to the elaboration and implementation of policies and activities to address external security threats to the EU in the area of cybersecurity, global cyberspace discussions and addressing cybercrime;
- provide interface and follow up with Commission, Council, EP and other relevant partners as well as with third parties in the areas mentioned above;

under the supervision of the Head of Cyber Policy Sector and Head of SECPOL3 Division.

Functions and Duties:

- Contribute to the elaboration and further development of EU policies and activities in the area of external security in particular in the area of cyber security
- Prepare and/or contribute to policy documents related to this area, in close cooperation with geographic services and with other institutions, member states and international organisations, as appropriate, including inter-institutional decision-making process
- Contribute to developing awareness and capacities within the EEAS and other services, provide policy guidance on global cyber issues
- Provide expertise to the EEAS SECPOL Cyber sector in the areas of International law, International Security, non-proliferation, and disarmament
- Contribute to the programming of the Instrument contributing to Stability and Peace (IcSP) as well as regional and bilateral instruments to address cyber security and cybercrime
- Seek to ensure coordination, complementarity and synergies with measures under other thematic and geographic instruments as well as with CFSP actions
- Establish and maintain regular contacts and exchanges with other EU institutions, Member States, third countries, public and/or private international organisations and/or with research institutions and the academic community at large in the area of responsibility
- Participate and/or represent the Division in meetings with stakeholders, including European Union institutions, Member States, third countries, international organisations and civil society at large.

Job Requirements

Education and Training: University diploma (International Law; International Relations; International Security)

Knowledge and Experience: Experience of at least 2 years in the abovementioned areas at institutional level, with analysis and reporting skills; knowledge of EU institutions, related decisional processes, CFSP, CSDP, International law, International Security, EU external action and related EU external policies;

Solid policy making experience and competence in one or more of the relevant fields: knowledge of the EU policy making processes and decision-making procedures; understanding of inter-relations in external and internal security dynamics, and relevant policy experience (e.g. International Law, International Security Policy, cyber security, Internet governance etc);

Have security clearance at minimal level SECRET EU[1], or undergo security vetting if s/he does not already hold security clearance at the appropriate level, in accordance with the relevant security provisions.

Skills

Linguistic skills: Have the capacity to work in the languages of CFSP and external relations necessary for the performance of the duties. (Thorough knowledge, capacity to write and speak, in English or French)

Communication skills: Capacity to work and communicate under time constraints in an international diplomatic and multilingual environment.

Ability to translate scientific or/and expert level information into input to policy papers and draft/make oral presentations in a synthetic manner;

Interpersonal skills: Ability to work professionally as a member of the unit, in taskforces and working groups with mixed composition; and willingness to travel frequently and at short notice;

To maintain the highest standards of personal integrity and impartiality. To exercise greatest discretion with regard to all facts and information coming to his/her knowledge in the course of or in connection with the performance of his/her duties.

Intellectual skills: Have strong organizational skills, ability to work under pressure within short deadlines and heavy workload and to manage multiple tasks and unexpected demands;

Solid analytical capability as well as drafting and reporting skills. Rapid grasp of problems and capacity to identify issues and solutions.

Personal Qualities

Dynamic. Motivated and flexible personality. Team-player. To adapt quickly to new situations and deal with new challenges.

---

[1]   SNE's or other external staff in the area of ESDP/CFSP may require access to EUCI and will in all likelihood require access to the EEAS Class I or Class II facilities. Access to such secure areas requires clearance to at least the level SECRET UE or national equivalent.