JOB DESCRIPTION FORM SNE
SECDEFPOL.1 - job no. 303211

I. IDENTIFICATION OF THE JOB

Type of post:	Seconded National Expert (cost-free)
Job title:	Policy Officer (Cybersecurity and cyber defence)
Function group and grade bracket:	
Entity:	Security and Defence Policy Directorate Security and Defence Policy Division – SECDEFPOL.1 Cyber Sector
Specialised post:	Yes
Security clearance:	SECRET EU

II. TASKS

The successful candidate will join the SECDEFPOL.1 Division's Cyber sector, and will contribute to the implementation of EU cyber diplomacy policy, notably through the implementation on the EU Cybersecurity Strategy, in consistent synergy with the Global Strategy and recent EU policy developments. The successful candidate does so through i.a. policy and concept development, analysis, context-specific technical advice, and knowledge management, working closely with Member States, EEAS geographical and relevant thematic services, EU Delegations, EUSR's, Special Envoys, CSDP structures, Commission services and international partners. Under the authority of the Head of the Security and Defence Policy Division and as part of the Cyber Sector, her/his main tasks will include:

Functions and Duties:

- Contribute to the elaboration and further development of EU cyber policies and activities, in particular in the areas of international (cyber) security, cyber defence, cybercrime and cyber capacity building;
- Prepare and/or contribute to policy documents related to this area, working closely with Member States, EEAS geographical and relevant thematic services, EU Delegations, EUSR's, Special Envoys, CSDP structures, international partners and Commission as well as other EU institutions, including through inter-institutional consultations and decision-making processes;
- Contribute to developing awareness and capacities within the EEAS and other services, mainstreaming cyber within the Common Foreign and Security Policy, providing policy guidance;
- Contribute to the implementation of the EU Cybersecurity Strategy;
- Contribute to the programming of the EU financial instruments to address cyber security, cyber diplomacy, cybercrime and cyber defence issues;
- Contribute to reports and briefings on activities in the area of responsibility;
- 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.

III. QUALIFICATIONS AND EXPERIENCE REQUIRED

- university diploma;
- Two years' relevant professional experience and ideally professional experience in multinational organisations;
- have experience and knowledge of CFSP and CSDP;
- relevant experience in areas of cybersecurity, cyber diplomacy, cyber defence and/or cybercrime;
- thorough knowledge of one EU working language and satisfactory knowledge of another one are required; in practical terms, in order to perform required duties, that means an excellent command of written and spoken English, in particular good report-writing skills; good knowledge of written and spoken French is desirable;
- good computer skills are essential, notably in word processing, spreadsheets, presentations software, Internet / Intranet and email systems. Knowledge of other IT tools would be an asset.

IV. CONDITIONS/ SKILLS REQUIRED

- have the ability to remain objective in complex scenarios and to display sensitivity and sound judgement;
- have good organisational skills, the ability to work under pressure and with tight deadlines and to manage multiple tasks and unexpected demands;
- have excellent drafting and communication skills;
- have excellent negotiating skills in a multinational environment;
- have the ability to work professionally as a member of the division, in mixed-composition task forces and working groups, in an interesting but challenging environment;
- maintain the highest standards of personal integrity, impartiality and self-discipline. The expert must exercise the greatest discretion with regard to all facts and information coming to his/her knowledge in the performance of his/her duties;
- national security clearance at SECRET UE level. Such clearance needs to be obtained from the competent authorities before secondment to the European External Action Service. It must be valid for the entire period of secondment. In its absence, the EEAS reserves the right to refuse the secondment as a national expert.

V. GENERAL CONDITIONS

National experts must be nationals of one of the Member States of the European Union and enjoy full rights as citizens.

The EEAS applies an equal opportunities policy.