Open Call for Consulting Services

Reference 024-018

TERMS OF REFERENCE: TECHNICAL ASSISTANCE – STUDY ON CYBER SECURITY AND ONLINE RADICALIZATION IN WESTERN BALKANS

Title:	Study on cyber security and online radicalization in the Western Balkans
RCC Department:	Political Department
Number of consultants :	1
Starting Date:	12 April 2018
Reporting to:	Head of Political Department
Location:	Sarajevo, Bosnia and Herzegovina
Duration:	12 April – 15 August 2018 (maximum 50 working days)
Application Deadline:	31 March 2018

I BACKGROUND

Purpose

The purpose of the consultancy is to assist the RCC in the implementation of commitments in the area of cyber security, as well as in the area of prevention and countering violent extremism, as defined by the RCC South East European Regional Platform for Countering Radicalization and Violent Extremism Leading to Terrorism and Recruitment of Foreign Terrorist Fighters (SEE Regional CVE-FTF Platform), and also the RCC's commitments as a partner in IPA II Regional Action on P/CVE in the Western Balkans.

The main expected output is a study which will provide a comprehensive overview and analysis of the situation as regards cyber security in: Albania, Bosnia and Hercegovina, Kosovo[*], Montenegro, Serbia and The Former Yugoslav Republic of Macedonia, (thereafter: WB6 economies). The study should elaborate the definition, legal and practical protection of critical infrastructure in WB6, legislation in force and the level of approximation with the EU respective acquis, development of institutional capacities, implementation of national strategies and challenges, operational national mechanisms in place and partnerships with private sector, academia and NGOs (to cover all WB6).

Recent actual cyber-attacks on critical infrastructure in SEE/WB, including their possible connections with terrorism and violent extremism should be listed and analysed, with lessons learned clearly delineated, as a part of preparations for future measures. Legal frameworks and practical challenges to effective cyber security in WB should be analysed. The study's conclusions should include clearly defined recommendation for further actions at both regional and national level. The study should also contain region-wide and jurisdiction-specific conclusions and recommendations for improvement of cyber security in WB6, including legal and practical measures to be taken at regional and national level to better define and protect critical infrastructure, counter cyber-attacks, and enhance prevention and countering online radicalization.

This should be done with the strong reference to countering online radicalisation and violent extremism that is leading to terrorism.

Background information

These days, the whole world is becoming more and more digitalised. The same goes for commerce, functioning of public administration and all governmental services, media, international relations, culture and entertainment. In fact, all aspects of contemporary life and especially human relations are already fully digitalised or are being digitalised at an increasing level.

This has been fully recognised by the European Union, which is in this area, at the global forefront. The EU Cyber Security Strategy was adopted in 2013, underlining the importance of cyber resilience, reducing cybercrime, development of cyber defence policy capabilities including industrial and technology resources. The Network Information Security Directive was adopted in 2016, while in September 2017 the European Commission adopted a cybersecurity package with new initiatives aimed to improve EU's cyber resilience, deterrence and defence. One of the proposals was to strengthen the European Union Agency for Network Information Security (ENISA).

South East Europe and in particular the Western Balkans is not lagging behind. First and foremost, technological and economic gap between the Western Europe and WB6 is far

[*] This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence

shallower in digital world than in general economy. The importance of digitalisation and cyber security has been recognised by the national governments in the region. The Western Balkans Six (WB6) leaders endorsed on 12 July 2017 the Multi-annual Action Plan for a Regional Economic Area (MAP) aiming to promote trade integration, introduce a dynamic regional investment space, facilitate regional mobility, and create a digital integration agenda. Trust and security and digital services, as one of the policy areas of the MAP, incorporates activities that aim to enhance cyber security, trust services and data protection. A Stocktaking and Need Assessment report is prepared by RCC Secretariat where major policy gaps and needs, including assistance through bilateral or regional projects are identified – detailed information on cyber security, trust services and data protection could be relevant for the purpose of this assignment.

In 2008, the SEECP Ministers of Foreign Affairs adopted a Common Declaration regarding the strengthening of cooperation in combatting cybercrime, agreeing to step up efforts at national and regional level in cyber security. The SEECP Bucharest Summit Declaration (June 2014) underlined the importance of intensified cooperation in the field of cyber security, as one of the most important challenges region is facing. It figured prominently on the agenda of 2017 Trieste Summit of the Berlin Process, and the same will be the case with the 2018 London Summit.

Digitalisation or "going online" offers great opportunities for sending, getting, gathering, and analysing information and therefore speeding up and facilitating journalists' work, scholarly research, business, public administration functioning and other areas of human work and life. At the same time, it greatly facilitates terrorist, criminal and other malevolent activities, such as:

- malicious cyber-attacks on virtual and digitalised "real life" critical infrastructure (ranging from messing up with civil status registries of citizens, disclosing classified information and sensitive personal data to disrupting the functioning of air, railway and road traffic and electricity supply systems);
- trade in illicit merchandise (weapons, drugs, human beings, stolen art, etc.) through Darknet, "regular" Internet or other electronic means;
- money laundering, fraud, extortion, and other financial criminal activities, including financing of terrorism and violent extremism;
- terrorist and violent extremist propaganda and misuse of social networks and online media for online radicalization.

The academic community and responsible authorities have started recognising the gravity of such threats at national, regional, European and global level, at both legal and practical plan. Much more, however, remains to be done, and a real and full view of the existing situation is the first step towards defining, planning and executing measures to improve prevention and countering of such illegal activities, threatening to seriously harm societies in WB6 and Europe as a whole.

II DESCRIPTION OF RESPONSIBILITIES

Objectives and Scope of Assignment

Building up on the existing mapping exercises and other relevant research and documents, the study should produce a comprehensive overview of actual and possible cyber-attacks on critical infrastructure in WB6 (including each and every of WB6), including their connections with terrorism and violent extremism. Legal frameworks and practical challenges to effective cyber security in WB6 should be analysed. The study's conclusions should include clearly defined recommendation for further actions at both regional and national level.

In particular, it should be done through keeping in mind the following axis pertinent to the overall regional cooperation in the field of expertise:

- legal definition and protection of critical infrastructure and services in each of the WB6;
- institutional capacities and adopted domestic cybersecurity strategies and related legislation within the framework of operational domestic mechanisms;
- partnerships with private sector, academia and NGOs in the development and implementation of cyber security policy;
- links between cyber security and countering terrorism and violent extremism in WB6 and strategic trajectories for boosting cyber resilience in the prevention of online radicalisation and violet extremism that is leading to terrorism.

The consultants (researchers) should pursue this research/study through:

- setting the theoretical and methodological framework for the research, and research plan;
- studying as thoroughly as possible available documents, case studies and other relevant scholarly and other available literature on the topic (desk research);
- doing fieldwork (interviewing relevant national and cyber security, as well as ICT experts);
- structuring and writing the study in a scholarly relevant way, yet understandable for wider interested audience;
- including specific conclusions and recommendations for relevant national authorities, but also regional organisations, especially the RCC.

The report should contain: (i) a brief narrative general introduction explaining the current level of the risk of cyber-attacks, other challenges to critical infrastructure and online radicalization, including its possible connection with planned or executed cyber-attacks; (ii) description of the situation in each of the WB6; (iii) identification of main challenges, vulnerabilities and needs for improvement; and (iv) conclusions and recommendations (general, for the RCC, and for the relevant national authorities).

The expert conducting the study should explore the needs and possibilities for inclusion of local communities into the cyber security raising awareness programmes for rehabilitation and reintegration of former FTF, terrorists and violent extremists in the Western Balkans. Conclusions and recommendations in this respect should be included in the report. Possibilities for inclusion of education in such programmes should also be researched and included in the study, especially as regards education and training for people participating in rehabilitation and reintegration programmes (whether imprisoned or not).

Tasks expected to be carried out

- Conduct a desk research on the state of play in the researched area (documents and available research - general background, European practices, functional and geographical).
- Conduct on-the-ground research in all six jurisdictions, with consultations at expert level, where needed, by travelling to the region (maximum thirteen trips – trips to be connected in a tour, if practicable, to lessen the time and financial resources used).
- Prepare the first outline, than the whole report, keeping to the schedule (deadlines) set by the RCC.
- Integrate any comments received from the RCC into the *final* version of the report.
- Fully adjust the final version with the RCC's Terminology/Nomination Guideline.
- Prepare the final version of the report.

The envisioned level of effort is set at a maximum of 50 (fifty) working days.

Deliverables

The following deliverables will be produced and transferred to the RCC during the course of the assignment:

- Outline of the report (introduction, structure and the methodology of the report) produced 20 calendar days after the commencement of the assignment.

- Draft of the whole report produced by 15 July 2018.

- Finalisation of the document expected 15 calendar days after receiving the final set of comments from the RCC.

- Presentation of the results to the RCC Board, SEE Group of National P/CVE Focal Points, and/or other bodies or meetings designated by the RCC and publishing of the report at the RCC websites and, if deemed necessary by the RCC Secretariat, in hard copy (brochure/book).

Timeframe

The total duration of the engagement will be approximately five months, starting on 12th April 2018 and finishing by 15th August 2018.

III COMPETENCIES

▪ University degree in political science, international relations, security studies, information and communication technology, or other appropriate field. Advanced degree with thesis directly related to the subject of engagement would be an advantage.
▪ Proven record of theoretical knowledge and practical experience and expertise in the areas described herein; minimum of 10 years of work experience, out of which 5 years of experience related to the scope of work; ▪ Demonstrable drafting skills; ▪ Proven analytical skills and ability to conceptualise and write concisely and clearly; ▪ Proven communication and presentation skills.
▪ Fluency in English, as the official language of the RCC. Knowledge of one or multiple languages of South East Europe would be an advantage.
▪ Familiarity with MS Office applications and in general with information and communication technology (ICT).

Core Competencies

- Expertise on cyber security as well as good background knowledge on matters related to prevention/countering terrorism and violent extremism (P/CVE). Expertise and good background knowledge on overall cyber security framework in the WB6, the EU and regional P/CVE framework;
- Demonstrates ability to establish good working relations with regional stakeholders ad respective EU authorities on these matters;
- Demonstrates professional competence to meet responsibilities and post-requirements and is conscientious and efficient in meeting commitments, observing deadlines and achieving results;
- Results-orientation: Plans and produces quality results to meet established goals, generates innovative and practical solutions to challenging situations;
- Communication: Excellent communication skills, including the ability to convey complex concepts and recommendations in a clear and persuasive style tailored to match different audiences;
- Team work: Ability to interact, establish and maintain effective working relations with a culturally diverse team; and
- Client orientation: Ability to establish and maintain productive partnerships with regional and national partners and stakeholders and pro-activeness in identifying the needs of beneficiaries and partners, as well as matching them to appropriate solutions.

Core Values

- Demonstrates integrity and fairness by modelling RCC values and ethical standards;
- Displays cultural, gender, religion, race, nationality and age sensitivity and adaptability.

IV QUALITY CONTROL

The expert should ensure an internal quality control during the implementing and reporting phase of the assignment. The quality control should ensure that the draft reports comply with the above requirements and meet adequate quality standards before sending them to stakeholders for comments. The quality control should ensure consistency and coherence between findings, conclusions and recommendations. It should also ensure that findings reported are duly substantiated and that conclusions are supported by relevant judgment criteria.

The views expressed in the report will be those of the contractor and will not necessarily reflect those of the Regional Cooperation Council. Therefore, a standard disclaimer reflecting this will be included in the report. In this regard, the expert may or may not accept comments and/or proposals for changes received during the above consultation process. However, when comments/proposals for changes are not agreed by the expert, he/she should clearly explain the reasons for his/her final decision in a comments table.

Quality Control by the Regional Cooperation Council

The consultant outputs shall be reviewed by the Regional Cooperation Council (RCC). The RCC may also engage one or more outside reviewers.

The final (second) draft shall be reviewed by the Regional Cooperation Council taking account of the previous comments made and how the expert has handled these comments. The approved final report will be subject to a quality assessment by the Political Department of the Regional Cooperation Council Secretariat, upon whose endorsement the report would be distributed and made public.

Relevant documents and useful links:

- http://www.rcc.int
- http://www.rcc.int/p-cve/

V APPLICATION RULES

Qualified candidates are invited to send an application via email to: ProcurementforRCC@rcc.int no later than 31 March 2018 Central European Time.

The consultancy will be awarded to the highest qualified applicant based on the skills, expertise and the quality of the concept note and the cost-effectiveness of the financial offer.

Only short listed candidates will be contacted

The application needs to contain the following:

- Letter of interest for the assignment;
- CV(s) including information on relevant knowledge and experience, as well as list of publications if applicable;
- Reference list including contact details (email addresses) of referees;
- An outline work programme of a maximum of 3 pages describing the main issues, a possible structure of the document, sources of information to be used, research tools to be employed by the consultant;
- Application Submission Form, Annex 1;
- Financial offer, Annex II.

When preparing the financial offer, the applicant should take into account the following:

- The proposed budget should include daily fee rate for consulting services; the fee rates should be broadly consistent with the EU framework rates for these types of professional services.

VI EVALUATION AND SELECTION

The application is evaluated on the basis of the profile and competencies of the candidate and the responsiveness to the Terms of Reference (ToR).

1. Profile and Competencies
2. Brief Concept Note
3. Financial evaluation based on Annex II

The best value for money is established by weighing technical quality against price on a 80/20 basis.

Technical Evaluation

EVALUATION GRID	Maximum score
Education	**30**
Qualifications and Skills Required	**30**
An Outline Work Programme	**30**
Language Skills	**10**
TOTAL SCORE	**100**

In addition to the results of the application, a competency-based interview will be held with the selected candidates.

Financial Evaluation

Financial Proposal/ cheapest price has maximum score	**100**

ANNEX I: APPLICATION SUBMISSION FORM

REF: 024-018 Open Call for Consultancy Services

One signed copy of this Application Submission Form must be supplied.

1 SUBMITTED by:

Name	
Surname	
Address	
Telephone	
Fax	
e-mail	

3 **DECLARATION**

[Name] _____ hereby declares that we have examined and accepted without reserve or restriction the entire contents of the Open Call for Consultancy -024-018

And we are not in one of the following situations:

(a) Bankrupt or being wound up, are having their affairs administered by the courts, have entered into an arrangement with creditors, have suspended business activities, are subject of proceedings concerning those matters, or are in any analogous situation arising from a similar procedure provided for in national legislation or regulations;

(b) Have been convicted of an offence concerning their professional conduct by a judgment which has the force of res judicata;

(c) Have been guilty of grave professional misconduct proven by any means which the Contracting Authority can justify;

(d) Have not fulfilled obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which they are established or with those of the country of the Contracting Authority or those of the country where the contract is to be performed;

(e) Have been the subject of a judgment which has the force of res judicata for fraud, corruption, involvement in a criminal organisation or any other illegal activity.

(f) Are civil servants or other agents of the public administration of the RCC Participants, regardless of the administrative situation, excluding us from being recruited as experts in contracts financed by the RCC Secretariat.

We offer to provide the services requested in the open call for consultancy on the basis of supplied documentation subject of this call, which comprise our technical offer and our financial offer.

Name and Surname	
Signature	
Date	

ANNEX II: BUDGET BREAKDOWN

REF: 024-018

No	Cost categories	Daily fee rate	Total Cost
2	**TOTAL COSTS**		
3	**VAT (if applicable):**		
	GRAND TOTAL (2+3):		

Proposed daily fee rate for consulting services should be broadly consistent with the EU framework rates for these types of professional services.