

INVITATION TO TENDER (AUSSCHREIBUNG ZUR ABGABE EINES ANGEBOTS)

public tendering procedure

Service: Technology Provider for Solution to Detect, Track and Mitigate Information Threats on the Internet

August 2023

About ISD

ISD is an organisation dedicated to understanding and countering hate, polarisation and extremism. We have a wealth of expertise in conducting research, analysis, and policy development to address the root causes of hate speech. For 17 years, we have worked across the hybridised threat landscape, combining expertise and action in weaponised hate, disinformation (state and non-state), conspiracy and extremism. This integrated threat perspective is critical in providing a comprehensive threat picture to our partners in driving a de-siloed response. We have unparalleled working relationships, cooperating and working with liberal democratic governments, international institutions at the senior levels, the media, and civil society and community organisations. In addition, ISD is very experienced using tech building on long standing cooperation with a variety of technology partners internationally.

Project context

Extremist and authoritarian communication and propaganda campaigns play a crucial role in shaping people's identities and undermining democratic norms and institutions. The Russian regime is working in the long term to undermine the Western alliance and its multilateral institutions, and therefore represents one of the key threats to democracy and human rights. As the Western Balkan countries are not yet fully integrated into European and transatlantic multilateral institutions, the region is an important target for Kremlin influence attempts. Both disinformation campaigns and support for anti-Western extremists are part of a broader, long-term strategy aimed at discrediting democratic institutions and undermining trust in the liberal international order.

There is therefore an urgent need for continuous digital analysis to identify pro-Kremlin dis- and misinformation targeting the Western Balkans. This will be used to inform policy makers, civil society and strategic communication efforts so that the Kremlin's attempts to influence the future direction of policy in the region can be countered.

Hence, ISD will record and analyse pro-Kremlin influence and disinformation campaigns in the Western Balkans. The focus will be on the Serbian language area (Serbia, but also Serbian-speaking communities in Montenegro and Republika Srpska) and Northern Macedonia. To do this, we will combine our in-house digital analysis team with the technology solution we are tendering here. The results of these analyses will be summarised in a research report of approximately 60 pages. In

addition, results will be made available to a wider audience through cooperation with media at home and abroad.

Based on the results of our research as well as the three typology working groups within this project, ISD will also create a typology of different disinformation threats.

Scope of work

To support the delivery of the project described above, the Institute for Strategic Dialogue will contract a service provider to develop and/or apply a highly specialised technology to detect, track and mitigate information threats on the Internet, for a project in the Balkans (Albanian, Russian, BCMS). This will involve tackling disinformation, covert state information operations, targeted hate campaigns and conspiracy narratives on various online platforms and websites.

ISD will take the lead in data analysis and communicating the findings to local level practitioners via its existing contacts, including briefing local level stakeholders, drawing upon the service provider for support and clarification where needed. Rigorous attention will be paid to ethical practice and guidance governing the sharing of findings beyond ISD and project partners, as well as data protection.

Working in close cooperation with the Digital Analysis Unit and analysts, the successful contractor will need to produce, in priority order, the following key deliverables across a 10-month project timeframe, starting in October 2023 and completed by the end of July 2024.

Service Description

The services required are outlined below across three distinct clusters:

Cluster One: Development

- a) Development and customisation of an environment to create “Architectures”, that live collect data from social media APIs
- b) Development of pipelines that leverage machine learning, natural language processing and statistical analysis to surface information threats
- c) Development of ‘early warning’ technology to identify disinformation messages and narratives likely to gain traction
- d) Create and maintain dashboards for ISD and local analysts to effectively investigate information threats in the analysed regions.
- e) Training of ISD staff in how to use the technology to conduct analysis, identify trends, and counter Russian disinformation in various geographies.
- f) Support the production and expansion of relevant seed lists in the analysed geographies.
- g) Support the identification of key platforms and outlets for the dissemination of Russian disinformation in the analysed geographies.

Cluster Two: Continuous Adaptation

- a) Daily/weekly data collection on multiple platforms based on the actor lists developed in Cluster One

- b) Integration of data in a system for near real-time tracking and classification of disinformation narratives.
- c) Integration of additional data sources relevant to the analysed geographies
- d) Development of pre-trained language models for text classification and named entity recognition in the examined languages.
- e) Reactive adaptation of the capability to improve the automated surfacing of information threats.
- f) Ensure adaptability to social media changes and ISD requirements.

Cluster Three: Maintenance and repairs

- a) Maintenance of hardware, including servers and server rooms.
- b) Data security, protection from data loss and data failures.
- c) Data backup, protection against data loss and data failures.
- d) Ensuring DSGVO compliance for data collection, storage and processing.

Technical specification

ISD is seeking to appoint a qualified contractor that bridges technology and research with substantial experience in the following areas:

1. Essential

- Experience in developing and adapting technology to combat disinformation and information threats on the Internet, with a focus on Russian disinformation.
- Proven track record of applying technology to various online platforms and countries.
- Ability to support analysis in the specified languages.
- Ability to support official API access to relevant social media platforms and news outlets.
- Expertise in leveraging natural language processing, machine learning, artificial intelligence, network analysis and data analytics to surface and combat information threats.
- Ability to reactively adapt the technology to changing requirements and social media landscapes.
- Working with a broad range of public sector organisations, including national and local governments in multiple countries;
- Building cooperative relationships with social media platforms and data holders; and
- Experience in data visualisation and creating user friendly interfaces to support data analysis.
- Proven track record delivering trainings

2. Desirable

- Existing ownership of and the ability to leverage a relevant software/ technology solution
- Experience working within multi-lingual and politically sensitive environments

Bid Evaluation Criteria

Proposals will be evaluated based upon the service to be provided weighed against the cost of the service. This will be done in line with ISD's Procurement Policy.

Factors that will be considered include:

- The responsiveness to the request for proposal and demonstrated understanding of ISD's requirements (10%)
- Experience and references of the service provider in similar projects (20%)
- Qualifications and subject expertise of the proposed team (20%)
- Quality and effectiveness of suggested technology and solutions (25%)
- Pricing and cost effectiveness of the proposal (25%)

Time frame

- Deadline for proposals: by the end of 28. Sep 2023
- to be submitted to verwaltung@isdglobal.org
- Form of proposals: maximum 20 pages in PDF Format in one file and/or 20 GB in one file
- Evaluation of proposals: 1-15 October 2023
- Announcement of the winner of the tender: October 2023

The delivery of the project is expected to last a total of 10 months, with contracting due to take place in October.

Bid submission requirements

All proposals should clearly state:

- Detailed description of proposed technology and solution.
- Timeline and fee for this work, inclusive of VAT or any other taxes or surcharges
- The contractors' qualifications as they relate to each of the criteria outlined above
- The contractors proposed personnel to conduct the activity with their one-page CVs
- Evidence of experience, references and qualifications.
- The proposal can be submitted in English or German

Any further questions can be sent to: verwaltung@isdglobal.org.

The total price for the service provided must not exceed €100,000.00. This amount is understood to be the net price. The statutory value added tax shall be shown separately.

€100,000.00 is the maximum net price available for this contract. However, ISD will be evaluating bids on the basis of their overall value for money and cost effectiveness. Bidders should craft their responses to meet the tender requirements and pursue value for money, not reach budget ceiling.

Contact

Institute for Strategic Dialogue gGmbH

Postfach 8 06 47 | 10006 Berlin | Germany

Verwaltung@isdglobal.org

Contractual arrangementsduration

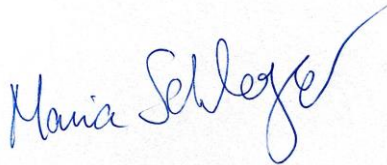
The contract will be awarded by ISD and will enter into force from the date of its signing by both parties, for the duration of the project until the satisfactory completion of all project deliverables and final reporting. The contract may be modified only through mutual agreement in writing signed by both Parties.

The contractor shall not disclose nor communicate any confidential information relating to ISD's business activities to any third party, save where required by law or with the express written consent of ISD. ISD reserves the right to terminate the contract if it finds that illegal or corrupt practices have taken place in connection with the contract award or submission.

The deliverables outlined in this tender may be subject to change, in line with § 47 of the German Regulation on Sub-Threshold Procurement (Unterschwel­lenvergabeordnung, UVgO), as required by the donor. Hence, §132 para. 2 of the German Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen, GWB) remains unaffected. The awarding of funding to the successful organisations by ISD is dependent upon ISD's receipt of funds from the donor.

The invitation to tender is subject to compliance with relevant legal provisions and regulations in connection with the award of services under the law on grants. The contracting authority reserves the right to reject bids or revoke the invitation to bid at any time.

Berlin, 26.08.2023



Ppa. Maria Schleußner
Head of Operations