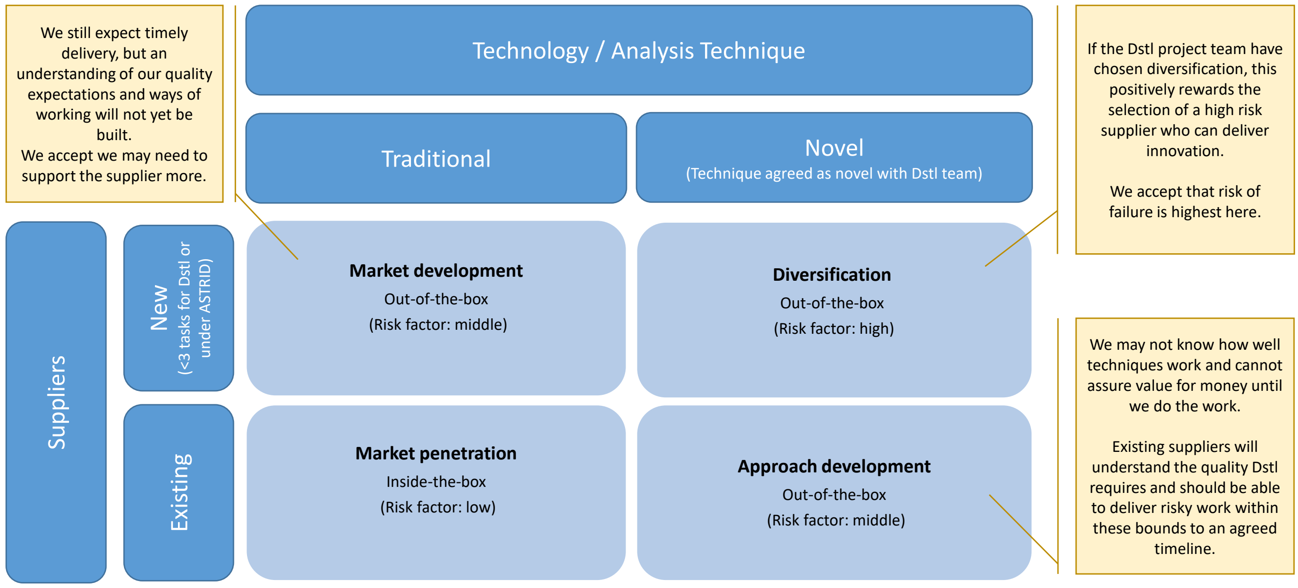
Statement of Requirement (SOR)

Contact & Project Information:

Project Manager	Name	**[Redacted under FOI exemption Personal Information]**		
	Email	**[Redacted under FOI exemption Personal Information]**		
	Telephone number	**[Redacted under FOI exemption Personal Information]**		
Technical Partner	Name	**[Redacted under FOI exemption Personal Information]**		
	Email	**[Redacted under FOI exemption Personal Information]**		
	Telephone number	**[Redacted under FOI exemption Personal Information]**		
iCas project number	[Redacted under FOI exemption Commercial Interest]			
Owning division	[Redacted under FOI exemption Commercial Interest]	**Delivering division**	[Redacted under FOI exemption Commercial Interest]	
Programme	[Redacted under FOI exemption Commercial Interest]			
Indicative task budget(s) £k	Core / initial work:	**[Redacted under FOI exemption Commercial Interest]**	Options / follow on work:	[Redacted under FOI exemption Commercial Interest]

Innovation risk appetite:	[Redacted under FOI exemption Commercial Interest]**Choose an item.**
Narrative (if applicable):	
Using the Ansoff matrix below, please indicate your risk appetite with regards to accepting innovative bids/solutions. The type of analysis/experimentation technique is included within 'Technology/Product'.	



We still expect timely delivery, but an understanding of our quality expectations and ways of working will not yet be built.
We accept we may need to support the supplier more.

If the Dstl project team have chosen diversification, this positively rewards the selection of a high risk supplier who can deliver innovation.

We accept that risk of failure is highest here.

We may not know how well techniques work and cannot assure value for money until we do the work.

Existing suppliers will understand the quality Dstl requires and should be able to deliver risky work within these bounds to an agreed timeline.

Use of Outputs: *(This section is used to inform risks, liabilities, mitigations and exploitation)*

Intended uses (including the approximate time before use and any key decisions that will use the output):

Produce a document to form a foundation for the rest of this project, so as to inform those things that AI tools could usefully help us discover concerning:

- Understand actions in, or that leave traces within, the Information Domain from the sub-threshold. So as to be able to identify which are, or appear to be: malign; accidental; and which are intended to reach out to us
- Increase the UK's ability to understand the implications and reach of its own defence activities in the sub-threshold
- Attribute actions to actors
- Identify likely or plausible intent or consequences
- Plausible response options

Possible uses:

Inform discussion with IRC partners.

Excluded uses:

Not Applicable.

Risk Assessment Process:

Project teams are required to complete the ASTRID Liabilities spreadsheet that will look at the direct and indirect risks associated with the work. The assessment must be completed at the outset before the draft SOR is submitted, this will prevent delays and lessen negotiations when the proposal is received. The risk assessment spreadsheet can be found in the document list on the: Some generic risks are pre-filled so please ensure they apply to your task and delete/add as necessary. Each risk must be assessed in turn and a score entered in the spreadsheet. They will be automatically marked and a colour code produced. Please enter the results in the boxes below. A completed copy of the spreadsheet must be attached to this SOR when submitting it to the for review and approval to release to CORDA.	
Direct Risk	[Redacted under FOI exemption Commercial Interest]
In the event that a direct risk is scored as “Green” or “Yellow” the risk will be capped at pre-agreed limits of liability and the project team may continue with the submission of their requirement to CORDA once all necessary approvals have been issued by the. In the event that a direct risk is identified as “Amber” or “Red” project teams should discuss the requirement with their Commercial POC before the task is submitted.	
Indirect/Consequential Risk	[Redacted under FOI exemption Commercial Interest]
In the event that the indirect risk is “Excluded” project teams may continue with the submission of their requirement to CORDA once all necessary approvals have been issued by the In the event that the indirect risk is identified as “Included” project teams should discuss their requirement with their Commercial POC before the task is submitted.	

Levels of Technical Assurance: The framework can offer three levels of Technical Assurance Support, and you have the ability to determine which level is suitable for your task. Full guidance listing the types of support under each level (and the trade-offs) can be found in the “ASTRID Guide – Levels of Assurer Support” or in the document list on the It may be that the level of support you require changes in the early discussion phase. Please ensure the final version of your SOR has the correct level indicated. Please indicate below which level you require		
Minimum ☐	Standard ☒	Enhanced ☐

Statement of Requirement (SoR)

Project's document ref	**AST075_Understanding_SubThreshold_SoR_v1.0_O**
Version number	**1.0**
Date	**16/09/2021**

1.	**Requirement**
1.1	**Title (including AST/ prefix)**
	AST/075_Understanding_SubThreshold
1.2	**Summary**

Context

This work is intended to set the foundations of understanding for a ‘generation after next’ future focused project. The overall purpose of this work is to enable Defence to do a better job, such that the ‘blood and treasure’ that is expended on behalf of the nation and our allies can have more nuanced effects in the dynamic adaptive world within which Defence operates.

This particular tasking focuses upon the sub-threshold, a world of constant competition short of war. Here, other actors directly engage through the Information Domain and / or leave traces of activity from other domain within the Information Domain. Our purpose is to understand actions in, or that leave traces within, the Information Domain from the sub-threshold. So as to be able to identify which are, or appear to be: malign; accidental; and which are intended to of friendly intent.

We recognise that what is being requested through **this** Statement of Requirement (SoR) **is a ‘big ask’**, noting both its scope and future focus, **but ask others to engage with us through ‘best efforts’ to jointly work to shape key decisions with us about how best to obtain a balanced product from this work, within the Limit of Liability.** Implied foundational questions include:

1) What is the Information Domain now;
2) What are actors directly doing in this domain, or doing that have the potential to leave traces in this domain, now (or have done recently (since 2008)), and
3) Then taking a perspective through the measured application of futurology. What does the Information Domain have the potential to *de facto* become, and when and by what potential stages and does this change the nature of what is done there or leaves traces there, or is it anticipated to more or less be the same in 15 – 30 years from now.

Tasking

This task will consider the span of the sub-threshold information domain, from which it will seek to understand the potential scope of actions in it, or that leave traces within it from actions in other domains. It is likely that this work will use a combination of top down thinking, concerning the scope that needs to be addressed, and middle out thinking concerning the structures within the information domain and the nature of potential traces of activity from other domains.

This work will seek to provide answers to the following questions:

1. What is the scope to focus on?

2. Where can the Machine Speed Strategic Analysis project add value?

3. How might AI be used to infer intent and evaluate plausible responses?

1.3	Background

Purpose

The Machine Speed Strategic Analysis (MSSA) project has been tasked with research to enable Defence to undertake ISR (Intelligence, Surveillance, and Reconnaissance) of the sub-threshold Information Domain. This is to enable Defence to process and understand the vast quantity of data that is there at machine speed and utilise advanced technology to identify action (or things leaving traces from actions in other domains), infer intent, and enable the evaluation of plausible calibrated responses. The desired outcome is to deliver demonstrators to improve the UK ability to:

- Understand actions in, or that leave traces within, the Information Domain from the sub-threshold. So as to be able to identify which are, or appear to be: malign; accidental; and which are intended to reach out to us;
- Increase the UK’s ability to understand the implications and reach of its own defence activities in the sub-threshold;
- Attribute actions to actors;
- Identify likely or plausible intent or consequences;
- Propose plausible response options.

The purpose of this EMR is to provide a base of knowledge from which the project team can understand the sub-threshold information domain, define research questions, and potentially identify routes to solutions.

Definitions

Sub-threshold: refers both to:

- The environment of constant competition, between state actors, in which sub-threshold activities are a primary means of seeking competitive advantage, and;
- The environment in which both states and others parties can seek to act in ways that produce a range of results (harmful, ‘less than friendly’, or ‘friendly’).

Sub-threshold activities: activities that are below the threshold of warfighting, and/or are below the threshold which would prompt a warfighting response from the target and its allies and partners.

Sub-threshold concept: refers to activities which are malign in their intent and/or effects with regard to the target’s objectives, interests, and values, and those of the target’s allies and partners.

Information domain: refers to a large and complex adaptive system comprising “*the information itself, the individuals, organisations, and systems that receive, process, and convey the information, and the cognitive processes that people employ, including the virtual and physical space in which this occurs.*”[1] For the purposes of this Statement of Requirements (SoR), the Information Domain includes both the active production of information, and the active or passive production of information ‘signatures’ through other activities (perhaps in other domains). Such things could include overt demonstrations of one state’s military capability deliberately, coincidentally, or accidentally producing fear and uncertainty among a neighbouring state’s population, but our view should not be limited to the actions of nation states, nor to things that necessarily harm.

Our definition of the Information Domain does not include the conduct of cyber operations, except where such operations produce a cognitive, rather than purely virtual, effect.

Sub-threshold information domain: the system within which:

- Indicators of other sub-threshold activity can potentially be found; such as information and indicators relating to the Salisbury attack in 2018
- Cognitive effects have the potential to result as passive by-products of other sub-threshold activity, such as intimidation of dissident voices
- Cognitive effects can also be more directly intended and potentially produced and experienced: such as interference with public voting intentions; or perhaps reaching out, in a manner intended to be friendly

Such effects can be driven by have the following span of intent:

- Harmful to the UK National Interest (or aspects thereof);
- Accidentally harmful to the UK National Interest (or aspects thereof), although this did not arise from any foundation in intent;
- ‘Less than friendly’ and seek to give others advantage at the expense of the UK National Interest (or aspects thereof);
- Accidentally ‘less than friendly’ to the UK National Interest (or aspects thereof), although this did not arise from any foundation in intent;
- Helpful to the UK National Interest (or aspects thereof), or at least seeking to reach out towards the UK and its interests in a way which is intended to be ‘friendly’;
- Accidentally ‘helpful’ to the UK National Interest (or aspects thereof).

[1] Development, Concepts and Doctrine Centre, *Allied Joint Publication-3.10.1: Allied Joint Doctrine for Psychological Operations: Edition B Version 1* (Brussels: NATO Standardisation Office, 2014), 1-1

1.4	**Requirement**
	The required output from this study is a comprehensive technical report, based upon reviews of existing literature and original research and analysis as appropriate. The purpose of this report is to answer the following questions: • What productive scope could follow-on work embrace? • Where can the MSSA project add value, through the understanding of the sub-threshold information domain at machine speed, to understand: ○ Actions in the sub-threshold, including the sub-threshold information domain; identifying which actions are, or appear to be, malign (noting that the cumulative result of actions in the sub-threshold, including the sub-threshold information domain could produce effects that are, or become malign) ○ The implications and reach of the UK's own defence activities in the sub-threshold ○ Attributing actions to actors ○ Identifying likely or plausible intent or consequences of the actions of actors; own, allied, and other ○ Plausible response options • **How might** Artificial intelligence (**AI**) **and** Machine Learning (**ML**) **be used to** conduct this work and to **infer intent** and **evaluate plausible responses at machine speed?** As part of the evidence provided by this report to answer these questions the report will explore and outline how the sub-threshold information domain has been observed to function, and be used by actors in pursuance of their sub-threshold intents, with a particular focus on areas of specific relevance to UK Defence. This should include: • The components of the system, including but not necessarily limited to: ○ The organisations responsible for directing sub-threshold activity ○ The producers, transmitters, amplifiers, and launderers of information ○ The activities which produce information ○ The information products and information 'signatures' themselves ○ The activities and intents sign-posted or signified by information

    - Target and collateral audiences, where this is the focus of intent
    - The second-order targets of cognitive effects (e.g. an individual or institution facing public hostility as a result of disinformation), and
    - The watchdogs and debunkers of misinformation and disinformation.

- How the system fits together, including where and how the components interact, and what cause-and-effect relationships can be observed or assumed between them.
- Multiplying and limiting factors acting within the system, where they are more or less predictable (e.g. predictable amplification by sympathetic audiences or the traditional media, vs. the less predictable nature of social media virality), and what factors may account for their strength or weakness.
- The ways in which an adversary might seek to keep their activity in the information domain, or the signatures of their activity reflected in the information domain, ambiguous and/or deniable.
- The tools and techniques and techniques that are or could be used to attribute such activities, and the challenges to effective attribution.
- The role of time in enabling, deploying, understanding, and countering malign activity and effects in or reflected in the sub-threshold information domain. What can be done quickly, what can currently only be done slowly, what trade-offs exist between time, cost, and effectiveness, and what challenges does this pose for all parts of the system and our response to it.
- The techniques and strategies that actors have been observed to use to deliver effect in the sub-threshold information domain.
- The known or assessed intents behind activity in the sub-threshold information domain, how they might be deduced from the activities and their effects, and any observed challenges to determining intent.
- Anticipated developments (e.g. technological advances, societal trends) over the next 5-10 years which could potentially have a significant impact upon any of the elements listed above.

Then taking a perspective through the measured application of futurology. Make an assessment of what the Information Domain has the potential to *de facto* become, and when and by what potential stages and does this change the nature of what is done there or leaves traces there, or is it anticipated to more or less be the same in 15 – 30 years from now.

With a view to the broader project's focus on the contribution that AI and ML at machine speeds can make to ISR, the report will note where indicators for any of the above might be found (and when (if the Information Domain is assessed to be evolving)), and the likely ease or difficulty with which the data might be gathered by manual or automatic collection processes. This should include not just direct indicators of activity, but also patterns which might indicate current or possible future activity (e.g. normalising that which should not be normal, gaining advantage that will affect the UK's future options or interests, also the creation of influential social media accounts and alternative media outlets which could act as amplifiers and launderers for future information activities). It should also consider indicators which cover not only known and previously observed activity, but which might also reflect signs that an actor is innovating in this space and pursuing approaches not seen before.

While the research and analysis is likely to be rooted in case studies with different instigators, audiences, and types of activity, the report should aim to identify commonalities where they exist, and note where differences observed in practice prevent a single understanding and where country- or issue-specific understandings are required.

The focus of case study-based literature reviews and research should primarily be on events from 2008 onwards, involving either the UK, its allies and partners, or third countries in which UK Defence is likely to have an interest.

While not intended to be prescriptive, the documents found at these links may serve as useful starting points:

- https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79
- https://www.rand.org/pubs/research_reports/RR2713.html
- https://stratcomcoe.org/publications/decoding-crimea-pinpointing-the-influence-strategies-of-modern-information-warfare/64
- https://nsiteam.com/social/wp-content/uploads/2019/04/Future-MI-CONOPS-and-ST-Roadmap-2035-2050_2-20-2019_FINAL.pdf
- https://www.hybridcoe.fi/

	Note: This statement of requirement uses systems language, but this is not intended to prescribe a systems-based approach to the task. **Task/Contract Management expectations** Fortnightly progress and technical reviews (telecoms) are expected as part of the delivery of this work. Close working and direction from the Dstl Technical Partner is required to ensure coherence with other MSSA project work undertaken in parallel.
1.5	**Options or follow on work**
	Not applicable

1.6	**Deliverables & Intellectual Property Rights (IPR)**						
Ref.	**Title**	**Due by**	**Format**	**TRL***	**Expected classification (subject to change)**	**What information is required in the deliverable**	**IPR DEFCON/ Condition** *(Commercial to enter later)*
D1	Kick-off Meeting	T0	Presentation (.pptx)	n/a	[Redacted under Military sensitive technical information exemption]	Presentation pack to include but not limited to: • Proposed delivery schedule • Review of risk management plan • Communications plan	
D2	Understanding the Sub-Threshold Information Domain Summary Report	24/01/2022	Report (.docx, pdf)	n/a	[Redacted under Military sensitive technical information exemption]	Comprehensive technical report, based upon reviews of existing literature and original research and analysis as appropriate.	DC705

D3	Recommendations for future requirements	24/01/2022	Report (.docx, pdf)	n/a	[Redacted under Military sensitive technical information exemption]	Report to focus on what productive scope could follow-on work embrace and where the MSSA project could add value.	DC703

*Technology Readiness Level required, if applicable

1.7	**Standard Deliverable Acceptance Criteria**
	Deliverable Acceptance Criteria (As per ASTRID Framework T&Cs) 1. Acceptance of Contract Deliverables produced under the Framework Agreement shall be by the owning Dstl or wider Government Project Manager, who shall have up to 30 calendar days to review and provide comments to the supplier. 2. Task report Deliverables shall be accepted according to the following criteria except where alternative acceptance criteria are agreed and articulated in specific Task Statements of Work: • All Reports included as Deliverables under the Contract e.g. Progress and/or Final Reports etc. must comply with the Defence Research Reports Specification (DRRS) which defines the requirements for the presentation, format and production of scientific and technical reports prepared for MoD. Reports shall be free from spelling and grammatical errors and shall be set out in accordance with the accepted Statement of Work for the Task. • Interim or Progress Reports: The report should detail, document, and summarise the results of work done during the period covered and shall be in sufficient detail to comprehensively explain the results achieved; substantive performance; a description of current substantive performance and any problems encountered and/or which may exist along with proposed corrective action. An explanation of any difference between planned progress and actual progress, why the differences have occurred, and if behind planned progress what corrective steps are planned. • Final Reports: shall describe the entire work performed under the Contract in sufficient detail to explain comprehensively the work undertaken and results achieved including all relevant technical details of any hardware, software, process or system developed there under. The technical detail shall be sufficient to permit independent reproduction of any such process or system. 3. Failure to comply with the above may result in the Authority rejecting the Deliverables and requesting re-work before final acceptance. 4. Acceptance criteria for non-report Deliverables shall be agreed for each Task and articulated in the Statement of Work provided by the Contractor
1.8	**Specific Deliverable Acceptance Criteria**

1.8.1 The Evidence Framework Approach (EFA)

The key deliverable from this work and its development shall be assessed through the lenses provided by the 'Evidence Framework Approach'. The top copy of the evidence framework approach is described in Glover and Pearce (2021).

1.8.1.1 Notes on the General approach to applying the (EFA)

Application of the EFA is not to be treated as a 'tick-box' exercise. If there is doubt the perspective for which there is doubt should be recorded as satisfying the lesser category of achievement, with discussion of why this is so, what would need to change to get a better assessment and how doable this is should a decision at some stage be made to apply additional resource and time

1.8.1.2 Assessing the Warrant of the Work

Warrant examines how good work is within the bounds that have been set for it in the SoR.

Assessment of the Warrant criteria is particularly helpful in supporting the practitioner team in the conduct of their work.

For details of how to assess Warrant see Glover and Pearce (2021).

1.8.1.2 Assessing the Validity of the Work

Questions of Validity examine the extent to which the work appears able to provide a framework to pick up activity in the Information Domain and usefully Interpret it through AI, either as an indicator of activity in other domains, or purely in terms of it serving to shape or fulfil intent within the information domain).

Such assessment supports the Red teaming of the analysis, which it would be useful to conduct within the project in collaboration with Dstl.

1.8.1.3 Assessing the Confidence of the Work

Questions of Confidence are assessed to support the next stages of Project Planning and provide a conceptual foundation for future years to support the AI community applying this perspective or these perspectives as the foundation for their work

References

	Glover, P & Pearce, P. (2020). Rapid assessment and review of simulation modelling. Journal of Simulation, Volume 14, 2020 issue 2. DOI:10.1080/17477778.2020.1757389

2.	Quality Control and Assurance
2.1	**Quality Control and Quality Assurance processes and standards that must be met by the contractor**
	☒ **ISO9001** (Quality Management Systems) ☐ **ISO14001** (Environment Management Systems) ☐ **ISO12207** (Systems and software engineering — software life cycle) ☐ **TickITPlus** (Integrated approach to software and IT development) ☐ **Other:** (Please specify)
2.2	**Safety, Environmental, Social, Ethical, Regulatory or Legislative aspects of the requirement**

3.	Security	
3.1	**Highest security classification**	
	Of the work	[Redacted under Military sensitive technical information exemption]
	Of the Deliverables/ Output	[Redacted under Military sensitive technical information exemption]
	Where the work requires more than occasional access to Dstl premises (e.g. for meetings), SC Clearance will be required.	
3.2	**Security Aspects Letter (SAL) – Note the ASTRID framework has an overarching SAL for quotation stage (up to OS)**	
	Not applicable If yes, please see SAL reference- *Enter iCAS requisition number once obtained*	
3.3	**Cyber Risk Level**	
	[Redacted under Military sensitive technical information exemption]	
3.4	**Cyber Risk Assessment (RA) Reference**	
	[Redacted under Military sensitive technical information exemption] This must be completed before a contract can be awarded. In accordance with the please complete the Cyber Risk Assessment available at	

4.	**Government Furnished Assets (GFA)**

GFA to be Issued - Choose an item.

If 'yes' – add details below. If 'supplier to specify' or 'no,' delete all cells below.

GFA No.	**Unique Identifier/ Serial No**	**Description:** *Classification, type of GFA (GFE for equipment for example), previous MOD Contracts and link to deliverables*	**Available Date**	**Issued by**	**Return or Disposal** *Please specify which*
GFA-1	ASC 0230 V1.0		From issue of SoR	PM	Disposal of copy issued
GFA-2			From issue of SoR	PM	Disposal of copy issued

If GFA is to be returned: It must be removed from supplier systems and returned to the Dstl Project Manager within 2 weeks of the final Task deliverable being accepted. (Any required encryption or measures can be found in the Security Aspects Letter associated with the Task).

If GFA is to be destroyed: It must be removed from supplier systems and destroyed. An email confirming destruction should be sent to the Dstl Project manager within 2 weeks of the final Task deliverable being accepted

5.	**Proposal Evaluation**
5.1	**Technical Evaluation Criteria**
	Process will be as per ASTRID Framework T&Cs. If particular attention should be paid to certain aspects of the requirement, please confirm here:
5.2	**Commercial Evaluation Criteria**
	As per ASTRID Framework T&Cs.