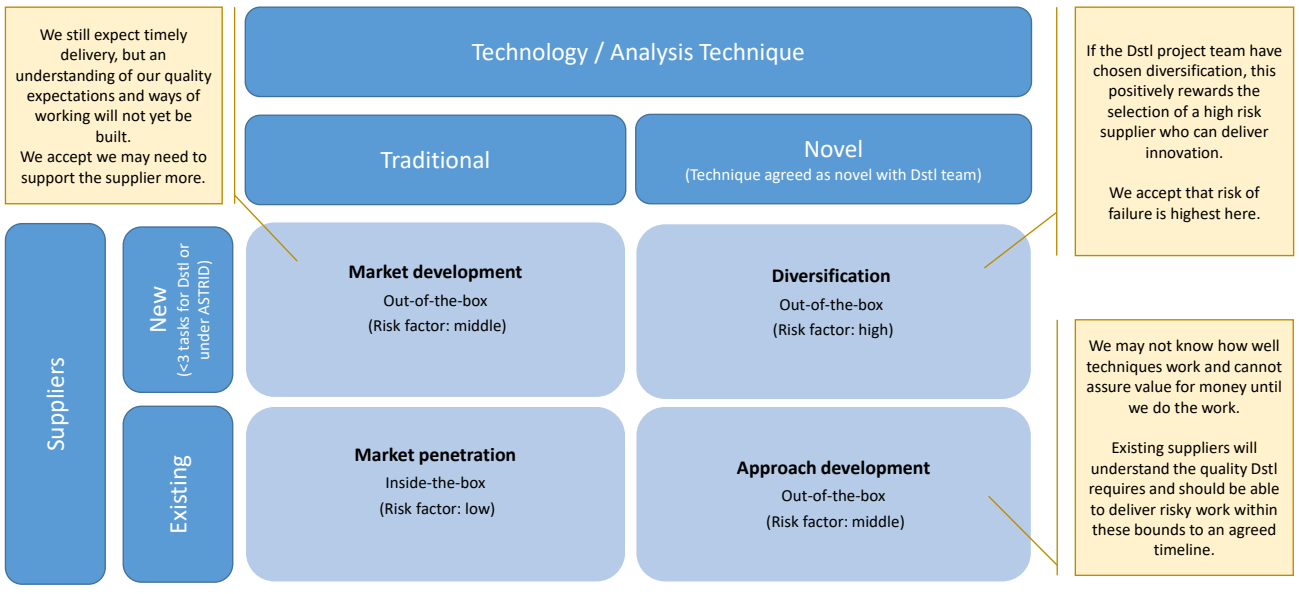
Statement of Requirement (SOR)

Contact & Project Information:

Project Manager	Name	Redacted under FOIA Section 40 – Personal information	
	Email	Redacted under FOIA Section 40 – Personal information	
	Telephone number	Redacted under FOIA Section 40 – Personal information	
Technical Partner	Name	Redacted under FOIA Section 40 – Personal information	
	Email	Redacted under FOIA Section 40 – Personal information	
	Telephone number	Redacted under FOIA Section 40 – Personal information	
iCas project number	709513		
Owning division	Exploration Division	**Delivering division**	Exploration Division
Programme	Policy & Capability Enterprise Support (PCES)		
Indicative task budget(s) £k	Core / initial work:	**£150**	Options / follow on work:

Innovation risk appetite:	Middle - Approach development
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'.



Use of Outputs:
This section is used to inform risks, liabilities, mitigations and exploitation. Questions 1-10 below should be a Yes/No/NA response. Please indicate if the questions do not make sense in the context of your task.
Intended uses (including the approximate time before use and any key decisions that will use the output):
Providing an immersive illustration of novel hybrid threats to policy officials and decision-makers to help guide thinking around the topic. This is not to support any specific decision, and these outputs will not be the sole such input. Providing a framework by which Dstl or MoD could use new inputs (e.g. technology horizon scanning products) to periodically review, update, and add to the vignettes.
Possible uses:
As a catalogue of pre-made vignettes for use in wargames or table-top exercises looking at hybrid threats.
Excluded uses:

1	Will any output be directly used as part of a safety critical system, or will it be one of the most important factors in decisions on Cat A/B investments (>£100M), or at Ministerial level policy making?	Redacted under FOIA Section 43 – Commercial Interest
2	Is this task collating and presenting previous work without making further / new recommendations?	
3	Is this task research - for example, an exploration of new methods, models or tools?	
4	Will a re-run of the modelling or analysis be required before outputs are presented to a decision maker?	
5	Will the outputs form a minor part of the work that will be combined by the Dstl Project Team before being used for decision-making?	
6	Has the approach to the work (how to undertake the work) been fixed by Dstl/MOD?	
7	Will 100% of the technical assurance of the outputs provided by the Dstl Project Team?	
8	Is the Dstl Project Team capping the maximum levels of verification and validation to be carried out on outputs?	
9	Is this task developing or maintaining a method, model or tool (MMT) which will be used for multiple use cases over a period of time by Dstl Project Teams?	
10	Can you confirm that there are no known intended uses of the outputs over and above those described here that could result in new risks if the output was incorrect?	

Statement of Requirement (SoR)

Project's document ref	**20211029-AST088_SoR_Novel_Hybrid_Threats v1.0**
Version number	**1.0**
Date	**29/10/2021**

1.	**Requirement**
1.1	**Title (including AST/ prefix)**
	AST088/Novel Hybrid Threats: Exploratory vignettes
1.2	**Summary**
	This work will provide an updatable collection of illustrative vignettes to inform policy officials and decision-makers about novel hybrid threats. It will do this by exploring current and anticipated trends, technologies, and capabilities in the context of listed components of hybrid threats.
1.3	**Background**
	The 2021 UK Defence Command Paper, *Defence in a Competitive Age*, describes an anticipated future out to 2030 characterised in part by systemic competition between states, including below the threshold of open warfare, and rapid technological change driving the acquisition of new capabilities by the UK's potential adversaries. The convergence of these realities raises the likelihood that the UK will experience novel forms of such below-the-threshold threats (henceforth referred to as 'hybrid threats'), whether targeted at the UK or at its allies and partners. Such novel hybrid threats might not bear a close resemblance to any hybrid threats previously experienced or observed (such as the seizure of Crimea, 2016-style election interference, or the NotPetya and Stuxnet cyberattacks). Along with the danger that they pose to their targets, the novelty of these threats gives them the potential to exert an additional disruptive and delaying effect upon UK Defence decision-making. [Redacted under FOIA Section 26 – Defence] For the purpose of this requirement, 'hybrid threats' refers to adversarial operations or campaigns by one state actor against another, utilising tools or methods beyond commonly accepted statecraft, to pursue an objective while intending to avoid a response above the threshold of armed conflict. 'Novel hybrid threats' refers to hybrid threats which represent a step-change from hybrid threats

	which have previously been observed in use, in terms of capability or the way that they achieve their effects or avoid detection, attribution, or countermeasures.

1.4	**Requirement**
	<u>Requirement #1: Project Generalities</u> The supplier must manage the project in order to deliver the work to high quality standards, on time and to budget. The supplier must nominate a suitably qualified and experienced Project Manager to control the execution of the project and manage the successful delivery of the project's outcomes. In their proposal, the supplier must: (i) generate a compliance matrix showing how it addresses each of these mandated requirements, and (ii) declare all areas of background Intellectual Property necessary to the successful delivery of the contract. During the contract, the supplier must monitor the project's progress, ensure any issues, risks or blockages in delivery are identified early and agree approaches with Dstl to mitigate them using a shared risk register. Monthly project management progress reports are to be prepared and e-mailed to the Dstl Project Manager and Technical Partner at the end of each month to cover the duration of the contract. It is anticipated that the monthly report will be a short document that covers: actions taken in response to meetings in the last month, meetings planned, key successes in the last month, current challenges, challenges likely to arise (informed by work undertaken to date), stakeholders engaged with, deliverables made / due, and updates to the risk register. Short monthly catch up meetings will also take place between Dstl, ASTRID and the supplier to track progress. A final technical report is to be delivered at the end of the contract. The scope and contents of the final report will be agreed with the Dstl Technical Partner ahead of the report being written. The final report should include the following: 1. Executive summary. 2. Introduction outlining the background, scope of work, approach and report structure. 3. Summary of the supplier's approach to the task including challenges identified before and during the project. 4. Detailed description of the work produced in response to the specific requirements of the task including vignettes illustrating novel hybrid threats. 5. Assessment of the approaches used by the supplier and discussion of lessons identified as a result of the work. 6. Aspects of the subject matter which might benefit from further examination. 7. Conclusions.

8. Appendices detailing any information used in support of point 4 above (as required).

In accordance with standard ASTRID T&Cs, Dstl will require 30 working days after report submission for review and for the supplier to implement corrections / changes, BEFORE final acceptance is confirmed. That said, Dstl will make best efforts to turn around in less, e.g. approximately 10 days.

The supplier will attend meetings either virtually, or in person if/when the Covid-19 lockdown period has been relaxed at Dstl Portsdown West, as required. These meetings will be arranged as appropriate.

Deliverables:

- Final Report. This must be delivered by NLT 08/03/2022.
- Dstl may require a study closure meeting/presentation, however, this will be determined as the study progresses.

Acceptance Criteria:

- Monthly progress reports must be delivered to Dstl on time and provide meaningful updates relating to the specifics of the project. Areas of progress and identified impediments to progress are to be made clear in these reports.
- Queries and questions raised by Dstl in relation to the content of the monthly reports are to be answered satisfactorily within 1 week of the monthly report to prevent work progressing in an unagreed manner which may deviate from the requirements.
- The final report is to be written in accordance with MOD report writing guidelines. The standard of writing, formatting, and presentation is to be of a professional standard.
- The final report will be reviewed by the Work Package Lead, Project Manager, Project Technical Authority and Lead Technical Reviewer.

Requirement #2: Project Specifics

The supplier will address the following points in a detailed, cohesive, and coherent manner to produce a report that provides a series of fictional yet plausible vignettes illustrating the use of novel hybrid threats in ways that bear relevance for UK Defence.

The programme of work should include (but not necessarily be limited to) these three steps:

1. Conduct a literature review to identify environments (e.g. the social media space/s), technologies (e.g. artificial intelligence), and capabilities (e.g. self-driving vehicles) which either exist today or are assessed as possibilities within a timeframe out to 2030. This might include multiple different directions in which a current technology or environment could evolve or be developed. This review should be broad-ranging and as detailed as required to provide the necessary inputs for Step 2. The focus should not be bounded at this stage by the immediate relevance for hybrid threats or for Defence.

2. Explore the implications of the identified elements in the context of the below list of components of hybrid threats. This list is indicative rather than fully prescriptive – the supplier is not restricted to it in either the breadth or the format of their analysis. Many of the examples given below relate to cyber and information activity, but again this is not prescriptive – the analysis should consider all domains and the interactions between them:
    a. **Activity.** What activities might be made possible and available to hybrid threat actors by the identified elements (e.g. harassment by swarming unmanned vehicles)?
    b. **Channel.** What new or evolved channels might activity be conducted through, and how might it change the possibilities available (e.g. a balkanised social media space allowing easy targeting of contradictory messages to different audiences)?

c. **Target.** What new or evolved elements might become plausible targets for hybrid threats (e.g. new generations of internet-connected appliances)?
d. **Target vulnerability.** How might targets become more vulnerable to hybrid threats, or vulnerable in different ways (e.g. unmanned/driverless vehicles being hacked, jammed, or spoofed in ways that human-driven vehicles could not be)?
e. **Effect.** How might an activity produce, either intentionally or not, new or different kinds of effects upon interaction with its target (e.g. a cyberattack triggering a cascading effect through a network of connected devices)?
f. **Enablers.** What new or evolved infrastructures might support novel forms of hybrid threat (e.g. quantum computing enabling rapid monitoring and evaluation of the effects of a hybrid threat)?
g. **Force multipliers.** What elements might exist to increase the effect of a hybrid threat (e.g. social media botnets-for-rent to amplify the outputs of an information operation)?
h. **Facilitating environment.** What new or evolved environments might be more conducive to hybrid threats (e.g. lightly-regulated information spaces permitting the circulation and reproduction of disinformation)
i. **Capacity.** What elements might increase the capacity of a hybrid threat actor (e.g. machine learning applications which allow the automated production of misinformation or disinformation rather than requiring human authors)?
j. **Speed.** What elements might increase the speed or responsiveness of hybrid threats (e.g. quantum computing enabling not only monitoring and evaluation of the effects of a hybrid threat, but also corresponding real-time adaptation of the activity)?
k. **Integration of effort.** What elements might allow hybrid threat actors to achieve better integration and coordination across domains/departments/levers of power (e.g. AI-assisted decision-making calibrating different inputs to cohere the most effective combination of activities)?
l. **Synergy of effects.** How might a hybrid threat actor be able to combine different activities to achieve a disproportionate effect when used in concert (e.g. inputting multiple activities into a hyperconnected digital environment to provoke a cascading reaction)?
m. **Ambiguity.** How might a hybrid threat actor be able to conceal the true nature of a threatening activity from its target (e.g. hiding a digital 'signal' in a mass of AI-created 'noise')
n. **Deniability.** How might a hybrid threat actor seek to avoid their actions being attributed to them (e.g. channelling funds to proxies through cryptocurrency to increase the anonymity of such transfers)?

3. Using the analytical output from the previous step, create no fewer than 9 fictional vignettes (see the vignettes in this report - https://www.csis.org/analysis/coping-surprise-great-power-conflicts - for an idea of what is desired) illustrating the use of novel hybrid threats in scenarios relevant to UK Defence. These may be against UK Defence targets, targets for which UK Defence has some responsibility, or targets which shape the environments within which UK Defence must operate. These vignettes should cover a range of RAND's categorisation of hybrid threats – Aggressive, Moderate, and Persistent (see page 3 - https://www.rand.org/pubs/research_reports/RR3142.html). They should not refer by name to real countries (except the UK), but can reflect real-world adversarial and alliance dynamics. Besides the core illustrative narrative, the vignettes should highlight:
    a. What, if any, specific objectives the novel hybrid threat might be used to pursue (i.e. what overarching effects the potential adversary might be seeking to achieve by this activity, without necessarily exploring their motivating grievances)
    b. If the novel hybrid threat uses new or evolved elements, what rough pathways might lead to their development
    c. The potential implications for UK Defence
    d. Any apparent countermeasures or resiliency options against each novel hybrid threat, whether they currently exist or are plausible by 2030 (given necessary investment)

	Deliverables: • Final Report as detailed in requirement #1. ***Acceptance Criteria:*** • The report must address each of the issues identified above with explanation as to the success or failure to do so.
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)*
D-1	Final Technical Report	4-March 2021	Report (.docx format)	n/a	Redacted under FOIA Section 26 – Defence	Report to include a description of the background, approach, data sources, analysis findings, conclusions and recommendations. Report should also include the 9 or more vignettes.	DEFCON 705 shall apply

*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**
	Not applicable

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 FOIA Section 26 – Defence
	Of the Deliverables/ Output	Redacted under FOIA Section 26 – Defence
	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)**	
	Redacted under FOIA Section 26 – Defence If yes, please see SAL reference- *Enter iCAS requisition number once obtained*	
3.3	**Cyber Risk Level**	
	Redacted under FOIA Section 26 – Defence	
3.4	**Cyber Risk Assessment (RA) Reference**	
	Redacted under FOIA Section 26 – Defence If stated, this must be completed by the contractor before a contract can be awarded. In accordance with the Supplier Cyber Protection Risk Assessment (RA) Workflow please complete the Cyber Risk Assessment available at https://suppliercyberprotection.service.xgov.uk/	

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					

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
5.2	Commercial Evaluation Criteria
	As per ASTRID Framework T&Cs.