RFI: **RFI-ACT-SACT-24-22- Cyberspace Warfare Development and Experimentation Campaign**

Reference: Q&A #1

Date of Issue: 18 March 2024

The following questions were raised with respect to subject **RFI-ACT-SACT-24-22-Cyberspace Warfare Development and Experimentation Campaign.** Responses are to provide clarification.

Questions	Responses
1. For RFI-ACT-SACT-24-22, how does HQ SACT define experimentation?	NATO Concept Development & Experimentation Handbook (available here) defines experimentation as "a controlled investigation to discover information, confirm or disprove a hypothesis, or formally validate (part of) a solution.
2. Can you share information or published news articles regarding previous experimentation conducted in support of the HQ SACT Cyberspace Warfare Development and Experimentation Campaign?	You can find on ACT website (here) an article about the 2023 cyberspace experimentation campaign. In the past, ACT conducted experiments in the areas of information sharing, operational-level Cyberspace Situational Awareness (CySA), information sharing, deception techniques or Autonomous Intelligent Cyber defence Agents (AICA), to name a few.
3. Is there a desired scope and scale for experiment proposals?	As mentioned in the RFI, the scope of the experiment proposals shall focus on concepts, solutions, and capabilities in support of cyberspace operations. The scale of the proposed experiment shall allow an in-year execution, which will only allow no or limited additional development, if so required.
4. Are there specific challenges or gaps within the topic areas identified that HQ SACT is particularly interested in addressing through experimentation?	The topics of particular interest are listed in the RFI (see para. 4.1).
5. Can you provide examples of constraints or limitations that might impact the feasibility or desirability of proposed experiments?	The proposed experiment shall be executable within a reasonable timeframe (about 4-6 months) and shall reuse an existing or under-development solutions/capability (i.e. no or limited additional development).
6. Are there common pitfalls or mistakes in submissions that respondents should avoid?	Submission of pure cybersecurity proposals at technical level or submission of proposals requiring extensive development to allow execution. Product/solution demonstration is also not considered as a valid experimentation effort.
7. Are there any specific AI technologies that HQ SACT is particularly interested in exploring for cyberspace operations?	AI technologies in support of CySA, Command-and-Control and decision support systems, to name a few.
8. Are there specific performance metrics or benchmarks that RFI responses should aim to meet?	The responses shall comply with RFI requirements, as stated in para. 4.2 (proposal formulated in terms of objectives/hypotheses/success criteria, focus on cyberspace domain operationalization, etc.).