Headquarters Supreme Allied Commander Transformation, Norfolk, Virginia

REQUEST FOR INFORMATION

RFI-ACT-SACT-25-22

This document contains a Request for Information (RFI) call to nations, industry and academia in support of 2025 HQ SACT cyberspace warfare development and experimentation campaign.

Nations, industry and academia wishing to respond to this RFI should read this document carefully and follow the guidance for responding.

General Information	
Request For Information No.	25-22
Project Title	Request for Information (RFI) call to nations, industry and academia in support of 2025 HQ SACT cyberspace warfare development and experimentation campaign.
Due date for questions concerning related information	**9:00 am EST, 6 March, 2025**
Due date for submission of requested information	**9:00 am EST, 4 April 2025**
Contracting Office Address	NATO, HQ Supreme Allied Commander Transformation (HQ SACT) Purchasing & Contracting Suite 100 7857 Blandy Rd, Norfolk, VA, 23511-2490
Contracting Points of Contact	1. Mr Robert Friend Email: Robert.friend@nato.int Tel: +1 757 747 4433 2. Ms. Catherine Giglio E-mail: catherine.giglio@nato.int Tel: +1 757 747 3856 3. Mr. Laurent Munster Email: laurent.munster@nato.int Tel: +1-757-747-3861
Technical Points of Contact	Name: Dr. Alberto Domingo E-mail: Alberto.Domingo@nato.int Tel: +1 757 747 3324 Name: Mr. Antoine Landry E-mail: antoine.landry@nato.int Tel: +1 757 747 3965
All request for clarifications, questions and responses to this RFI must be sent via email to all Points of Contacts reported above. Individuals email will not be accepted and should not be sent. Contracting and Technical POCs must be included in any correspondence.	

1. INTRODUCTION

1.1. HQ SACT is issuing this RFI to engage with nations, industry and academia. The objective is to identify existing and under-development cyberspace operations concepts, products or capabilities which HQ SACT can consider for warfare development and experimentation in support of NATO cyberspace operations.

➔ **This RFI is seeking innovative, tailored and actionable experiment proposals in the area of cyberspace operations to inform HQ SACT cyberspace warfare and capability development efforts. Generic proposals to demonstrate, validate or evaluate commercial product will not be considered.**

1.2. This RFI does not constitute a commitment to issue a future Request for Proposal (RFP). This is not a formal request for submissions as part of a procurement. The purpose of this general request is to invite and involve nations, industry and academia through collaboration to help identify existing or under-development concepts, products or capabilities to inform the cyberspace domain development activities. HQ SACT has not made a commitment to procure any of the items described herein, and release of this RFI shall not be construed as such a commitment, nor as authorization to incur cost for which reimbursement will be required or sought.

1.3. Further, respondents are advised that HQ SACT will not pay for any information or administrative costs incurred in responding to this RFI. The costs for responding to this RFI shall be borne solely by the responding party. Not responding to this RFI does not preclude participation in any subsequent RFP if issued in the future. All information shared with HQ SACT might be shared with contracted third parties in order to support the capability development process as needed. Provision of data, or lack of, will not prejudice any respondent in the event that there is a competitive bidding process later as part of NATO Common-Funded Capability Development.

2. BACKGROUND

2.1. By declaring cyberspace as an operational domain, NATO recognizes that conducting operations in or through cyberspace contributes to the success of the mission in a manner like those executed in the traditional domains. This recognition broadens the former approach, limited to defending NATO Communication and Information Systems (CIS) infrastructure, to a wider set of functions required to integrate cyber components into operations and missions.

2.2. Consequently, there are areas where NATO has a very clear understanding of what must be done as a result of the recognition of cyberspace as a domain of operations, however, the how to do it, and what are the required concepts, products or capabilities are constantly evolving. Conversely, there are other aspects which are innovative and introduce new warfighting dimensions that are not yet fully understood and which cannot be easily adapted from existing domains.

3. PROJECT DESCRIPTION

3.1. Vision

3.1.1. As demonstrated by recent military conflicts (e.g., Russia's war of aggression against Ukraine), daily criminal activities or even the Covid-19 pandemic, cyberspace remains a vehicle of choice for attackers. Meanwhile, digital society's increasing reliance on technology makes it more susceptible to manipulation, influence, and attacks through cyberspace.

3.1.2. In this increasingly diverse, complex, quickly evolving, and demanding security environment, and beyond pure cybersecurity/CIS security activities, NATO needs to be able to operate in cyberspace as effectively as it does in the traditional domains, alongside relevant civilian and military stakeholders. This includes the development and maintenance of operational-level Cyberspace Situational Awareness (CySA), the execution of effective Cyberspace Command-and-Control (C2) and the development of robust and realistic Education, Training, Exercise and Evaluation (ETEE) solutions for cyber operators, to name a few.

3.1.3. In this context, HQ SACT – NATO warfare development command – is responsible for leading cyberspace transformation, ranging from cyberspace concept definition to capability development. As explained above, a particular emphasis is put on cyberspace operations, as opposed to traditional cybersecurity/CIS security.

3.2. Objectives

3.2.1. As part of cyberspace transformation, warfare development and experimentation play a key role to test and explore concepts, products or capabilities with a view to speeding up the delivery of critical cyberspace capabilities to warfighters. To support cyberspace transformation through experimentation – and notably feed the development of cyberspace operational capabilities – NATO needs to get a comprehensive overview of existing and under development concepts, products, or capabilities.

3.2.2. This RFI is intended to provide nations, industry and academia with an opportunity to share with HQ SACT experiment proposals related to their existing and planned concepts, products, or capabilities in the area of cyberspace operations.

3.3. Expected Benefits to Respondents

3.3.1. Nations, industry and academia will have the opportunity to inform and shape HQ SACT cyberspace warfare and capability development activities, which can result in potential collaboration opportunities (e.g. experiments as part of NATO's flagship exercise Cyber Coalition). Working with HQ SACT on this project will contribute to increased visibility and international promotion of your solutions, while helping respondents understand and focus efforts on essential

cyberspace capabilities, which are needed to operationalize the cyberspace domain.

3.4. Expected Benefits to NATO

3.4.1. By identifying experiment proposals related to innovative and forward-looking concepts, products or capabilities in the area of cyberspace operations, HQ SACT will feed cyberspace transformation, notably through experimentation, with a view to delivering, at the time of relevance, cyberspace operations capabilities to NATO warfighters. Through this effort, NATO expects to rationalize efforts, encourage synergies, improve interoperability and creates Communities of Interest (CoI).

4. REQUESTED INFORMATION

- ➔ **HQ SACT is inviting nations, industry and academia to submit a white paper containing experiment proposals related to existing or under-development cyberspace operations concepts, products or capabilities.**

- ➔ **Cyberspace operations include defensive, offensive and cyber intelligence operations, and utilize enablers like Cyberspace C2, CySA, decision-support solutions, and cyberspace operations ETEE. These are the areas of interest of ACT, for the purposes of this RFI.**

- ➔ **Cyberspace operations are underpinned by strong cybersecurity. However, cybersecurity is not in the scope of this RFI. Similarly, Information Operations (IO), Electromagnetic Spectrum Operations (EMSO), Space technology/operations and overall Operational C2 are related but focus solely on these areas (without linkages to cyber) are not in the scope of this RFI.**

- ➔ **Responding to this RFI requires effort and resources. Please do not respond to this RFI if:**
  - **The proposal is about demonstrating a product or technology.**
  - **The proposal is in the area of cybersecurity (technical-level) concepts, products and technologies, which are of use for the service providers and cybersecurity centers, but not for the operational staff or the commander.**
  - **The concept, product or technology cannot be tailored to NATO policy, doctrine or requirements in cyberspace operations.**
  - **The concept, product or technology is on a related area of interest (e.g., cognitive warfare, information operations, electromagnetic spectrum, information environment, etc.) but is not sufficiently linked to cyberspace operations.**

4.1. White Papers – topics/area of interest. Whilst fostering the cybersecurity and resilience of CIS infrastructure and networks remains key, HQ SACT focuses efforts on the continuous development of the **Cyberspace Domain at military/mission-level**. HQ SACT therefore seeks concepts, products or capabilities addressing the

key functions, operations and enablers, as described in the table below. Potential experimentation areas of interest are also mentioned. However, this **list is not all encompassing**. HQ SACT is open to experiment proposal(s) addressing other novel ideas, concepts, products, or capabilities that can feed HQ SACT cyberspace transformation efforts.

Cyber function/ operation/ enabler	Description	Potential experimentation areas of interest
Cyberspace Situational Awareness (CySA)	This refers to the need to develop and maintain CySA at the operational level, combining cyberspace threat awareness, network/CIS awareness and mission awareness to inform Commanders' decision-making. ➔ Building on the successful 2024's experimentation campaign on CySA processes and products, which informs the procurement of NATO Cyberspace Situational Awareness System (CySAS), HQ SACT is more particularly interested in **decision support concepts and technologies** to augment CySAS.	• Risk models to calculate total risk to tasks/objectives/mission. • Cyber contribution to mission assurance. • Course of Action (CoA) generation, evaluation and management (with quantifiable impact on task/mission assurance, thus enabling objective and efficient decision making). • Automatic ingestion of threat reports including mapping to the mission, service, and threat data models to inform the CySA products. • Automatic ingestion of Operation Plans (OPLANs) and Operation Orders (OPORDs) to generate mission operational designs. • Artificial Intelligence (AI) tools in support of the above activities and processes.
Cyberspace Command & Control (C2)	Overall C2 refers to the Commander's need to maintain effective decision-making and execution of operations and ensure that effects delivered in or through different domains are orchestrated to achieve mission objectives. By recognizing Cyberspace as a Domain, cyberspace should be fully integrated into existing Multi-Domain Operations (MDO) and the overall C2 functions.	• Cyber C2 system analysis and design. • Mission decomposition and analysis for cyber and multi-domain missions. • Tools in support of Cyber C2 processes (RFI, targeting process, order generation and management, etc.). • CoA analysis and evaluation (including "What-if scenario" development). • Cyber effects modelling, cyber effect orchestration. • Joint- and multi/cross/all-domain operations. • AI tools in support of the above activities and processes.

Education, Training, Exercises and Evaluations (ETEE)	This refers to the need to enable the force, through ETEE solutions, to know how to operate together and then to execute in concert with one another cyberspace operations.	• Digital twins and synthetic environments. • Cyberspace operational-level scenarios allowing the modelling and simulation of theaters of operations, actors, CoA, effects, etc. • Cyber Range Digital Library and related management and orchestration systems. • Strategic and operational level war-games.
Cyberspace Intelligence, Reconnaissance, Surveillance (CyISR)	This refers to activities whereby intelligence is derived in or through cyberspace.	• Cyber Threat Intelligence (CTI) integration into CySA. • CyISR collection, fusion and dissemination. • CyISR integration into intelligence lifecycle. • AI tools in support of the above activities and processes.
Defensive Cyber Operations (DCO)	This refers to defensive actions in or through cyberspace to preserve friendly freedom of action in cyberspace.	• Resilience and mission assurance frameworks. • Operational-level deception techniques to inform military-level CySA (*note: sole technical-level deception is not in scope*).
Offensive Cyber Operations (OCO)	This refers to activities in or through cyberspace that project power to create effects which achieve military objectives.	• OCO integration into joint targeting. • Operational risk analysis. • De-confliction mechanisms. • Battle Damage Assessment (BDA). • AI tools in support of the above activities and processes.
Cyber Multi-Domain Operation Integration	This refers to the need to integrate and orchestrate military activities across all operating domains and environments, while ensuring synchronization with non-military activities and stakeholders. As cyberspace is a domain mainly owned and operated by commercial providers, fostering civilian-military collaboration is essential.	• Integration of cyberspace operations into information/cognitive warfare operations. • Civilian-military integration. • Cross-domain/cross command information sharing.

Emerging and under-development concepts	This includes experiments that support warfare development efforts and elicitation and identification of capabilities in the most current HQ SACT's Warfare Development Agenda (WDA).	• Cyberspace integration with Electronic Warfare (EW). • Cyberspace support to Cognitive Warfare, MDO and Digital Transformation.
Innovative solutions and key enablers	This notably refers to the use of Emerging and Disruptive Technologies (EDTs), provided that proper use cases in support of cyberspace operations can be articulated. AI technologies as it relates to Cyberspace Operations may include Natural Language Processing (NLP), data correlation/prediction/ prioritizations/orchestrations, process automation/ augmentation that ultimately free cyberspace operators for more strategic tasks.	• AI in support of CySA and/or Cyber C2 development. • AI-supported data repository in support of CySA data collection, thus harvesting multiple sources through automated mapping, correlation and fusion, summarization and apportionment of risk to the different mission elements, services and threats. • Language models to ingest format free information. • Generation and evaluation of alternative CoAs that may leverage a selection of services/units/time sequences to provide a human operator with a menu of options to maximize cyber contribution to mission assurance. • Homomorphic encryption.

4.2. White Papers – format

4.2.1. The white paper shall address, at a minimum, the following:

a) **Experiment proposal(s)** formulated in terms of objectives, hypotheses, success criteria, technical set up, metrics, etc.
b) **Brief description** (maturity, use cases, etc.) of the concept, product or capability to be experimented with.
c) **Effort/cost (ROM[1])** required to conduct the proposed experiment.
d) **Other relevant information**, including constraints or limitation related to the experiment proposal.
e) **Designated point(s) of contact** (name, phone, e-mail).

➔ **This RFI is seeking innovative, tailored and actionable experiment proposals in the area of Cyberspace Operations to inform HQ SACT cyberspace warfare and capability development efforts.**

➔ **Responding to this RFI requires effort and resources. Please do not respond to this RFI if:**

- **The proposal is about demonstrating a product or technology.**
- **The proposal is in the area of cybersecurity (technical-level) concepts, products and technologies, which are of use for the service providers and cybersecurity centers, but not for the operational staff or the commander.**
- **The concept, product or technology cannot be tailored to NATO policy, doctrine or requirements in cyberspace operations.**
- **The concept, product or technology is on a related area of interest (e.g., cognitive warfare, information operations, electro-magnetic spectrum, information environment, etc.) but is not sufficiently linked to cyberspace operations.**

➔ **HQ SACT will exceptionally consider concept development and experimentation design short studies and research efforts, should be the topic be of primary relevance for HQ SACT and the maturity of the experiment requires a preliminary research phase.**

4.2.2. Responses to this RFI **shall not be classified above NATO UNCLASSIFIED.**

4.2.3. The white paper (main document and enclosures) should not exceed **10 pages**. It should be single-spaced, have one-inch margins, assume US letter-size (8 1/2 by 11 inches) page, use 12-point font, and be formatted for compatibility with Microsoft Word or Adobe Acrobat Reader (current versions).

[1] HQ SACT seeks non-binding Rough Order Magnitude (ROM) price estimates for the sole purpose of estimating programmatic costs and planning funding for future program proposals/bids. Provision of data, or lack of, will not prejudice any respondent in the event that there is a competitive bidding process later on, as part of NATO Budget and NATO Common Funded Capability Development policies.

4.2.4. Submissions should be named according to the following convention: <Respondent company name; maximum of 12 characters>_CYBER-EXP-RFI_<date in YYYYMMDD format>.<filename extension of 3 or 4 characters>.

4.2.5. The response(s) to this RFI shall be submitted by e-mail. Submissions must include both the Contracting and Technical POCs listed on page 2. The responses shall not contain proprietary and/or classified information. HQ SACT reserves the right to seek clarification on submissions.

4.2.6. Eligibility to Respond. Only NATO nations, and industry and academia that originate or are chartered/incorporated within NATO nations are eligible to respond to this RFI. Companies from Partner Nations who want to participate should collaborate with a primary company headquartered within a NATO Nation.

4.2.7. Respondents can collaborate with other providers, but all companies/organizations must be clearly identified and their role/services clearly stated.

4.2.8. The information may be considered in developing any future potential Statement of Work requirements. HQ SACT will consider selected information for developmental contracts and experimentation candidates.

➔ **Please note that HQ SACT intends to invite a selected number of RFI respondents to a cyberspace warfare development and experimentation workshop to present their proposal and engage with the NATO/Allies operational community. This event is expected to take place in June 2025.**

4.3. Response Due Date. Responses to this RFI must be received by **9:00 am EST 4 April 2025**. The responses shall not contain any classified information. HQ SACT reserves the right to seek clarification on submissions.

5. CLARIFICATIONS AND QUESTIONS

5.1. All questions should be submitted by e-mail solely to the aforementioned POCs by **9:00 am EST 7 March, 2025** to allow for appropriate response time prior to the **9:00 am EST 4 April 2025** response due date.

5.2. Accordingly, questions in an e-mail shall not contain proprietary and/or classified information. Answers will be posted as soon as possible on the HQ SACT P&C website at: https://www.act.nato.int/opportunities/contracting/

6. ADDITIONAL INFORMATION

6.1. Non-disclosure Principles and/or Non-disclosure Agreement (NDA) with Third Party Company.

6.1.1. Please be informed that HQ SACT may contract a company to conduct investigation or analysis in support of this project. HQ SACT will follow

nondisclosure principles and possibly conclude an NDA with that company to protect submitted information from further disclosure. As the third-party beneficiary of this nondisclosure, this RFI serves to inform you how HQ SACT plans to proceed and HQ SACT's intent to protect information from unauthorized disclosure. This requires the third-party company to protect the disclosed information using the highest degree of care that the company utilizes to protect its own Proprietary Information of a similar nature, and no less than reasonable care.

6.1.2. The third-party company receiving the information shall not, without explicit, written consent of HQ SACT:

a) Discuss, disclose, publish or disseminate any Proprietary Information received or accessed under nondisclosure principles and subject to an NDA, if an NDA is concluded;
b) Use disclosed Proprietary Information in any way except for the purpose for which it was disclosed in furtherance of the goals of the instant project, collaboration, activity or contract; or
c) Mention the other Party or disclose the relationship including, without limitation, in marketing materials, presentations, press releases or interview.

6.2. Organizational Conflicts of Interest.

6.2.1. As Procurement/Contracting involves the expenditure of funds allocated by the member nations, we must always strive to maintain trust in and preserve the integrity of the procurement procedures. It is essential that our procedures facilitate transparent and robust competition from industry.

6.2.2. Contractor and subcontractor personnel performing work under an HQ SACT contract may receive, have access to, or participate in the development of sensitive information relating to source selection methodology, cost or pricing information, budget information, and future specifications, requirements or Statements of Work or perform evaluation services that may create a current or subsequent Organizational Conflict of Interests (OCI). Similarly, companies responding to an HQ SACT RFI may create a subsequent OCI determination when pursuing future NATO contracts generated from that RFI.

6.2.3. Each individual contracting situation will of course be examined on the basis of its particular facts and the nature of any proposed contract. The exercise of common sense, good judgment, and sound discretion is required in both the decision on whether a significant potential conflict exists and, if it does, the development of an appropriate means for resolving it.

6.2.4. In anticipation of a future OCI determination, any company either awarded an HQ SACT contract or responding to an HQ SACT RFI while also anticipating bidding on future NATO contracts relating to this work, should consider having a mitigation plan in place to address or mitigate any OCI concerns now or in the future.

6.3. Handling of Proprietary Information. Proprietary information, if any, should be minimized and clearly marked as such. HQ SACT will treat proprietary information with the same due care as the command treats its own proprietary information. HQ SACT will exercise due care to prevent its unauthorized disclosure. Please be advised that all submissions become HQ SACT property and will not be returned.

6.4 Exceptions to Obligations. The third-party company receiving the information may disclose, publish, disseminate, and use Proprietary Information:

a) To its employees, officers, directors, contractors, and affiliates of the recipient who have a need to know and who have an organizational code of conduct or written agreement with the recipient requiring them to treat the disclosed Proprietary Information in accordance with nondisclosure principles and the NDA (if executed);
b) To the extent required by law; however, the company receiving the information will give HQ SACT prompt notice to allow HQ SACT a reasonable opportunity to obtain a protective order or otherwise protect the disclosed information through legal process that is:
   - demonstrated in written record to have been developed independently, or
   - already in the possession of the company receiving the information without obligation of confidentiality, prior to the date of receipt from HQ SACT, or
   - disclosed or used with prior written approval from HQ SACT, or
   - obtained from a source other than HQ SACT without obligation of confidentiality; or publicly available when received.

6.5. Any response to this RFI is considered to establish consent to this process. A copy of the NDA, if or when concluded, can be provided on request.

7. SUMMARY. This is a RFI only. The purpose of this RFI is to involve nations, industry and academia through collaboration to collect experiment proposals to feed cyberspace transformation. HQ SACT has not made a commitment to procure any of the items described herein, and release of this RFI shall not be construed as such a commitment, nor as authorization to incur cost for which reimbursement will be required or sought. It is emphasized that this is a RFI, and not a RFP of any kind.

***