Headquarters Supreme Allied Commander Transformation Norfolk Virginia

REQUEST FOR INFORMATION
RFI-ACT-SACT-23-16

This document contains a Request for Information (RFI) call to industry, academia and nations in support of a political and military-strategic level wargame to assess NATO's scope of cyberspace operations, coordination and collaboration processes needed.

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

HQ Supreme Allied Commander Transformation RFI 23-16 General Information	
Request For Information No.	23-16
Project Title	Request for Information (RFI) to industry, academia and nations in support of a political and military-strategic level wargame to assess NATO's scope of cyberspace operations, coordination and collaboration processes.
Due date for questions concerning related information	9:00 am EST 13 March 2023
Due date for submission of requested information	9:00 am EST 24 March 2023
Contracting Office Address	NATO, HQ Supreme Allied Commander Transformation (SACT) Purchasing & Contracting Suite 100 7857 Blandy Rd, Norfolk, VA, 23511-2490
Contracting Points of Contact	Ms Magdalena Ornat Email: magdalena.ornat@act.nato.int Tel: +1-757-747-3150 Ms Tonya Bonilla E-mail: tonya.bonilla@act.nato.int Tel: +1 757 747 3575 Ms Catherine Giglio E-mail: catherine.giglio@act.nato.int Tel:+1 757 747 3856
Technical Points of Contact	Maj Ugur UYSAL, E-mail: ugur.uysal@act.nato.int Tel: +1 757 747 3994
All request for clarifications and responses to this RFI must be sent via email to all Points of Contact reported above.	

RFI-ACT-SACT-23-16

1. Introduction

Summary. Headquarters Supreme Allied Commander Transformation (HQ SACT) is issuing this Request for Information (RFI) in order to engage with industry, academia and nations. The objective is to identify existing and under-development industrial/commercial/academic concepts, products, or capabilities which NATO could consider towards the utilization of a political and military strategic level **wargame**[1] on cyberspace operations, coordination and collaboration processes needed using the latest technical support possibilities, such as Augmented Reality and Simulation. HQ SACT is seeking comprehensive support for the wargame, including the design, development, execution, analysis, and reporting.

This RFI does not constitute a commitment to issue a future Request for Proposal (RFP). The purpose of this request is to involve industry, academia and nations through collaboration, in an examination of existing and under-development concepts, products or capabilities to assess NATO's scope of cyberspace operations, coordination and collaboration processes needed with a political and military strategic level wargame. 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.

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 ACT 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. Description of the Programme (Cyberspace Wargame)

Cyberspace is contested at all times. NATO and its allies rely on strong and resilient cyber defences to fulfil the alliance's core tasks of collective defence, crisis management and cooperative security. The Cyberspace domain contributes effects achieved in and through Cyberspace to Multi-Domain-Operations (MDO). In order to achieve these effects, stakeholder coordination and collaboration in and beyond the Military Instrument of Power are required. To allow NATO to further adapt to the evolving cyber threat landscape and implement Cyberspace as a domain of operations, NATO's scope of cyberspace operations, coordination and collaboration processes shall be assessed on both political and military strategic levels through wargaming. The aim is to inform the operationalization of the Cyberspace domain and NATO Cyberspace capability development. HQ SACT plans on organizing such a Cyberspace Wargame in 2023/2024. The main target audience for the Cyberspace

[1] NATO proposed definition of wargaming: The application of scenario based models in a safe-to-fail environment in which the outcome and sequence of events affect, and are affected by the decisions made by the players (two or more opposing sides).

Wargame are the high-rank decision-makers at the political consultation and strategic communities in NATO. Test runs for the Cyberspace Wargame are planned to be executed within HQ SACT or other NATO entities.

The Cyberspace Wargame will **aim** to:

- Provide NATO policymakers with information and insights to assess the scope of the Cyberspace domain, coordination and collaboration processes needed.
- Promote collective decision-making and problem-solving within the Cyberspace domain on NATO's political and military strategic level.
- Depict possible limitations constituted through NATO's current doctrine, policy, guidance, processes and capabilities in the Cyberspace domain using realistic threat scenarios.
- Identify possible adjustments in doctrine, policy, guidance, processes and capabilities that enables the Alliance to defend itself in Cyberspace as effectively as it does in Air, on Land, and at Sea.
- Inform the NATO Cyberspace capability development.

Applicable policies and directives:

- Military Vision: In his vision for NATO 2030, the Secretary General stressed that "NATO needs to be as politically ready as it is militarily. As such, it should institute a practice of periodic wargaming, net assessment presentations, and threat scenarios in the North Atlantic Council (NAC) and/or Military Committee (MC), incorporating new data techniques and technologies in visualisation."
- Allied Joint Publication (AJP)-3.20, Allied Joint Doctrine for Cyberspace Operations, is the NATO doctrine to plan, execute and assess Cyberspace Operations (CO) in the context of Allied joint operations. AJP-3.20 is a part of NATO's operations architecture and derives its authority from and complements AJP-3, Allied Joint Doctrine for the Conduct of Operations.
- NATO policy on cyber defence: At the 2021 NATO Summit in Brussels, Allies endorsed a new Comprehensive Cyber Defence Policy, which supports NATO's three core tasks of collective defence, crisis management and cooperative security, as well as its overall deterrence and defence posture. NATO's defensive mandate was reaffirmed, and Allies committed to employing the full range of capabilities to actively deter, defend against and counter the full spectrum of cyber threats at all times. Responses need to be continuous and draw on elements of the entire NATO toolbox that include political, diplomatic and military tools. Allies also recognised that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as an armed attack. The nature of cyberspace requires a comprehensive approach through unity of effort at the political, military and technical levels.

Applicable roles, responsibilities and authorities:

- The NAC is the principal political decision-making body within NATO. It oversees the political and military process relating to security issues affecting the whole Alliance. It brings together representatives of each member country to discuss policy or operational questions requiring collective decisions, providing a forum for wide-ranging consultation between members on all issues affecting their peace and security.

- The MC is the primary source of military advice to NATO's civilian decision-making bodies – the NAC and the Nuclear Planning Group. The MC provides military guidance and advisement to the Alliance's two Strategic Commanders and participates in developing overall strategic policy and concepts. The MC prepares an annual long-term assessment of the strength and capabilities of countries, and areas posing a risk to NATO's interests. The MC represents an essential link between the political decision-making process and the military structure of NATO.

- The Supreme Allied Commander Europe (SACEUR) is responsible for the overall command of NATO military operations. He conducts the necessary military planning for operations, including the identification of forces required for the mission and requests these forces from NATO countries, as authorised by the NAC and as directed by the MC. SACEUR analyses these operational needs in cooperation with the SACT.

3. Scope of Capability (Cyberspace Wargame)

Within the Cyberspace Wargame, the aim is to support decision-making to ensure enablement of agile and critical thinking to maintain NATO's competitive edge in the Cyberspace domain. The Cyberspace Wargame should be executed according to the applicable policies, directives, roles, responsibilities, and authorities**.** For example, consider the following scenario: the NAC is requested to make a decision on whether to activate a mission upon a NATO member nation calling for Article 5 after a massive cyber-attack on their infrastructure. The NAC should decide on the mission mandate. SACEUR should plan for a number of Cyberspace Operations, support deployment of Cyber Rapid Response Teams (CRRTs), as authorised by the NAC and as directed by the MC.

HQ SACT is open to entertaining other novel ideas, concepts, products or capabilities withal recommendations addressing potential needs to the Cyberspace Wargame, and a clear proposal on how NATO could apply the solutions. The scope of the Cyberspace Wargame should meet the following minimum requirements, noting the list below is not comprehensive:

The Cyberspace Wargame should:

- Be based on a realistic cyberspace threat scenario.

- Focus on the political and military strategic levels in order to reveal and inform the nature of political and military challenges emerging in a cyber-war against threats faced by NATO.

- Allow for the assessment of existing processes to coordinate and collaborate between the respective relevant military and non-military stakeholders for the specific threat scenario.

- Allow to wargame multiple threat based scenarios (which stimulate varying workflows) to harden process related findings.

- Include focus beyond Cybersecurity (CS) and also consider Defensive Cyberspace Operations (DCO) and the coordination and collation needed for Offensive Cyberspace Operations (OCO[2]) within the alliance, as well as Cyber Information, Surveillance and Reconnaissance (CISR).

- Place particular emphasis on time-relevant decision-making of NATO in the Cyberspace domain.

- Employ state of the art technologies to support the execution of the Cyberspace Wargame.

4. Requested Information and Response Guidelines:

HQ SACT is inviting industry, academia and nations to submit comprehensive information on existing and under-development concepts, products or capabilities in the area of Cyberspace wargaming on the political/military-strategic level or wargames on either of the two areas (cyberspace, political/military-strategic level), that would allow to develop a wargame sufficing the scope or contribute to specific areas of the scope.

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

Response Due Date: Responses to this RFI must be received by **9:00 p.m. EST on 24 March 2023.**

The information shall be presented in **Microsoft Word for Office compatible format**, and shall not contain classified information. The information shall address, at a minimum, the following:

- Type of proposal (idea/concept/product/capability);

- Purpose;

- Brief description, which should include the following phases:
  - Design: How should the Cyberspace wargame be designed to produce the insights and information needed to achieve the aims? What is the estimated timeframe?

[2] Under current policy, NATO itself is not authorized to conduct offensive cyber operations. Instead NATO relies on "Sovereign Cyber Effects Provided Voluntarily by Allies" (SCEPVA).

  - Development: How should virtual environments, simulations, and other technologies and materials support the wargame to achieve the aims? What is the estimated timeframe?

  - Execution: How should the wargame be executed and how should the wargame players be led towards achieving the aim of the wargame?

  - Analysis: How should the wargame be analysed and how should the insightful contributions of the wargame players be captured? Lessons identified from the wargame must be captured; how is this done?

  - Reporting: How should the results be reported, including the main insights of the wargame and the conclusions for NATO's Cyberspace Operations?

- Examples of potential use for the scenario as described in sections 2 and 3.

- Brief description if a product/idea/concept is mature with applicable tooling available, or if parts of the solution are still under development.

- When applicable, brief description of effort/cost requirement to finalize its implementation/adaption/adoption.

- Other relevant information, including constraints or limitation to the adoption of the proposal by NATO, e.g. Intellectual Property Rights, Export control regulations/International Traffic in Arms Regulations, etc.

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

5. Presentation.

HQ SACT may ask selected RFI respondents to provide a presentation based on their submission. Selected RFI respondents may be given the opportunity to present their submission during the spring 2023 Think-Tank for Information Decision and Execution Superiority (TIDE) Sprint Conference[3] in Lillehammer (NOR) from 17 to 21 April 2023. The cyberspace wargame session is scheduled for 19 APR 2023, which will include a creative workshop regarding the design and development of the cyberspace wargame.

6. Clarifications and Questions

Inquiries of a technical nature about this RFI shall be submitted by e-mail solely to the aforementioned POCs by 9:00 am EST **13 March 2023**. 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://act.nato.int/contracting.

[3] Spring 2023 TIDE Sprint registration link: https://cvent.me/XV9BQa

7. Organizational Conflicts of Interest.

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 this Headquarters' procurement procedures. It is essential that our procedures facilitate transparent and robust competition from industry.

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.

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.

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.

8. 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.

9. Non-disclosure principles and/or nondisclosure agreement (NDA) with third party company.

HQ SACT will follow non-disclosure principles and possibly conclude an NDA with any companies to protect submitted information from further disclosure. As the third party beneficiary of this nondisclosure, this RFI serves to inform you of how HQ SACT plans to proceed and of HQ SACT's intent to protect information from unauthorized disclosure, requiring 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. This includes the following responsibilities and obligations:

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

- Discuss, disclose, publish or disseminate any Proprietary Information received or accessed under nondisclosure principles and subject to an NDA, if an NDA is concluded;

- 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

- Mention the other Party or disclose the relationship including, without limitation, in marketing materials, presentations, press releases or interviews.

10. Exceptions to Obligations

The third party company receiving the information may disclose, publish, disseminate, and use Proprietary Information:

- 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);

- 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; or

- 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; that is disclosed or used with prior written approval from HQ SACT; obtained from a source other than HQ SACT without obligation of confidentiality; or publicly available when received.

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.

11. Questions

Questions of any nature, including technical ones, about this RFI announcement shall be submitted by e-mail solely to the contracting and technical POCs. Accordingly, questions in an e-mail shall not contain proprietary and/or classified information. Answers to questions will be posted, for everyone’s awareness, on the HQ SACT P&C website at: www.act.nato.int/contracting.

12. Summary.

This is a RFI only. The purpose of this RFI is to involve industry, academia and nations through collaboration, in an examination of existing and underdevelopment ideas/concepts/products and capabilities to assess NATO’s scope of Cyberspace Domain including reviewing doctrine, policy, guidance, processes and capabilities with a wargame on the political and military strategic level. 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 emphasised that this is a RFI, and not a RFP of any kind. All responses to this RFI should be received no later than **24 March 2023.**