Headquarters Supreme Allied Commander Transformation (HQ SACT), Norfolk, Virginia

REQUEST FOR INFORMATION (RFI) 2026
HQ SACT Cyberspace Warfare Development & Experimentation Campaign

RFI-ACT-SACT-26-26

This document contains a Request for Information (RFI) call to nations, industry and academia in support of:

2026 HQ SACT Cyberspace Warfare Development & Experimentation Campaign

NATO and National organizations, 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.	26-26
Project Title	Request for Information (RFI) call to nations, industry and academia in support of 2026 HQ SACT cyberspace warfare development and experimentation campaign.
Due date for questions concerning related information	**9:00 am EST, 27 February, 2026**
Due date for submission of requested information	**9:00 pm EST, 20 March 2026**
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	Ms. Catherine Giglio E-mail: catherine.giglio@nato.int Tel: +1 757 747 3856 Mrs. Inga Love Email: inga.love@nato.int Tel: +1 757 747 4231
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 requests for clarification, 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 that 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 products will not be considered.
- ➔ Proposals related to cyber security of systems, services and information will not be considered. Only proposals applicable to operations in cyberspace and supporting capabilities will be considered.
- ➔ Generic proposals that do not result in a tangible product (demonstrator, minimum viable product, concept, etc.) will not be considered.

1.2. This RFI does not constitute a commitment to issue a future Request for Proposal (RFP). This notice is not a formal request for submissions as part of a procurement. The purpose of this general request is to invite nations, engage with industry and academia through collaboration to help identify existing and under-development concepts, products or capabilities to inform 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 the existing (physical) 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) or daily criminal activities, cyberspace remains a vehicle of choice for attackers. Meanwhile, society's increasing reliance on digital technologies 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 mission-level[1] Cyberspace Situational Awareness (CySA), the execution of effective Cyberspace Command-and-Control (CyC2) and the development of robust and realistic Education, Training, Exercise and Evaluation (ETEE) solutions for cyber operators, to name a few. Those cyberspace functions and capabilities are also essential in order to implement Multi-Domain Operations (MDO[2]).

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, with a view to enabling MDO at military/mission-level.

3.2. Objectives

3.2.1. As part of cyberspace transformation, warfare development and experimentation play a key role in testing and exploring concepts, products or capabilities to speed 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, supported by constantly evolving technologies.

3.2.2. This RFI is intended to provide nations, industry and academia with an

[1] Mission-level refers to activities in the strategic, operational and tactical domains, and for the purpose of this RFI exclude cyber security / technical activities. Cyber-security/technical activities are considered out of the scope of this RFI, and will not be considered.
[2] See: https://www.act.nato.int/activities/multi-domain-operations/

opportunity to share with HQ SACT proposals related to their existing and planned concepts, products, or capabilities that might be considered or adopted for NATO cyberspace operations.

3.3. Expected Benefits to Respondents

3.3.1. Nations, industry and academia 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 increase visibility and international recognition of your solutions, while helping respondents understand NATO's needs and priorities in terms of cyberspace operations capabilities. On a strictly non-committal basis, HQ SACT may explore the possibility of allocating limited funding in the future to support the development of ideas, products, or capabilities related to the scope of this RFI.

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 expediting the delivery of cyberspace operations capabilities to NATO warfighters. Through this effort, NATO expects to rationalize efforts, encourage synergies, improve interoperability and create Communities of Interest (CoI).

4. REQUESTED INFORMATION

4.1. Scope Clarification

- ➔ HQ SACT is inviting nations, industry and academia to submit a white paper containing experiment proposals related to existing and under-development cyberspace operations concepts, products or capabilities at military/mission-level.
- ➔ Cyberspace operations include Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO) and Cyberspace Intelligence, Reconnaissance, Surveillance (CyISR) operations. Enablers include CySA, CyC2, decision-support, and ETEE solutions including emerging technologies such as Artificial Intelligence (AI). Both cyberspace operations and associated enablers are areas of interest of ACT for this RFI.
- ➔ Cyberspace operations are underpinned by strong cybersecurity. However, cybersecurity is not in the scope of this RFI. Similarly, Information Operations (IO), Electromagnetic Operations (EMO), space technologies/operations and overall operational Command and Control (C2) are of interest but lack of deep linkage to cyberspace operations will prevent them from being considered for this RFI.
- ➔ Responding to this RFI requires effort and resources. Please DO NOT respond to this RFI if:

- The proposal is about demonstrating a commercial 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 commanders.
- The proposed concept, product or capability does not align with NATO policy, doctrine, or requirements in cyberspace operations.
- The concept, product or capability is on a related area of interest (e.g., cognitive warfare, IO, EMO, etc.) but is not sufficiently linked to cyberspace operations.
- The proposal is on the area of AI but is not detailed enough to assess its feasibility/interest, or if it requires large amounts of training data, which for sensitivity issues cannot be made available.

4.2. White Papers – Topics & Areas of Interest. HQ SACT seeks concepts, products or capabilities addressing the key functions, operations, and enablers, as described in the table below.

Areas of particular interest for 2026 include:

- ✓ **Cyberspace operations ontologies** (i.e., practical applications of their use).
- ✓ **Alliance-wide CyC2** functions and processes (e.g., for own and adversarial Course of Action – CoA – generation and analysis, dynamic force management, opportunity development and analysis, decision support, etc.).
- ✓ **Operational-level adversarial picture** production and dissemination in support of CySA, CyC2 and Cyber Resilience. Technical (network/service-level) adversarial pictures are out of scope.
- ✓ **Cyber effects (direct and indirect[3])** integration[4], in particular as part of **joint and MDO planning and targeting** processes or as **Cyber Identity Armies** as instruments of national influence that can achieve strategic effects.
- ✓ **AI solutions and tools (potentially** including **Graph Retrieval-Augmented Generation (RAG), Recursive and Adaptive RAG or Agentic AI, and AI-enabled rapid software development and prototyping of cyber C2 systems)** in support of cyberspace tasks and processes at the operational/military level (i.e., planning, execution, assessment of missions). AI solutions and tools in support of technical-level tasks and processes (e.g., real-time network monitoring) are out of scope.

➔ *Please note that the list below **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.*

[3] As defined in AJP 3.20, Allied Joint Doctrine for Cyberspace Operations: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

[4] In accordance with NTAO policy, the development of cyber effects is out of scope of this RFI. The integration in the C2 processes of third-party provided cyber effects is the core interest for this RFI.

Cyber function/ operation/ enabler	Description	Potential experimentation areas of interest
Cyberspace operations ontologies	Ontologies create structures for information and allow data integration and enhanced exploitation, while revealing gaps in knowledge. While there are several ontologies for cyber security, there are still not widely approved ontologies for cyberspace operations.	• Development of cyberspace operations ontologies in support of data integration and exploitation. • Validation of ontologies using simple tools for information sharing. • Validation of ontologies using simple tools for data exploitation. • Demonstration of practical tools to implement and exploit ontologies.
Cyberspace Situational Awareness (CySA)	This refers to the development and maintenance of CySA at the operational level, combining cyberspace threat awareness, network/CIS awareness, and mission awareness to inform Commanders' decision-making. ➔ NATO Cyberspace Situational Awareness System (CySAS) has entered the acquisition phase. HQ SACT is therefore ONLY interested at this stage in **decision support concepts and technologies (including AI)** to augment CySAS.	• Cyber contribution to mission assurance. • Mission Assurance-Based Cyber Resilience (MACR), beyond Military Instruments of Power (MIoP) – e.g., interconnection with Critical National Infrastructure (CNI). • Automatic ingestion (i.e., AI solutions and tools) of mission data (Operation Plans (OPLANs), Operation Orders (OPORDs), etc.), threat data (including mapping to services and activities) and network/service data to rapidly feed CySAS. • AI solutions and tools to enhance and exploit the mission operational design data – for instance by building/generating information cards associated with each node with information on dependencies, vulnerabilities, threats, etc. • AI solutions and tools to support the automatic generation of CySA products (operational pictures, situational reports, commander's briefs, RFI, etc.).

		• Cyber mission portal generation, ingesting CySAS diverse data and providing, via additional outputs such as infographic and diagrams, enhanced comprehension and projection capabilities.AI solutions and tools to support other CySA-related activities and processes.
Cyberspace Command & Control (CyC2)	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 of operations, cyberspace should be fully integrated into existing MDO and the overall C2 functions.	• CyC2 Information System (CyC2IS) analysis and design, covering mission planning, execution, assessment, etc. • Mission decomposition and analysis for cyber and multi-domain missions. • Tools in support of CyC2 processes (RFI, targeting process, order generation and management, force management, etc.). • CoA generation, evaluation and management (with quantifiable impact on task/mission assurance, thus enabling objective and efficient decision making). • Simulation solutions and tools for CoA analysis and evaluation (including "What-if scenario" development). • Cyber effects modelling and cyber effect orchestration. • AI solutions and 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 at tactical, operational and strategic level together then to execute cyberspace operations in concert with one another.	• Mission/operation level digital twins and synthetic environments. • Cyberspace operational-level (audacious/train-as-you fight) scenarios allowing the modelling and simulation of theaters of operations, missions, actors (including red and purple teams), CoA, effects, etc. • Cyber Range Digital Library and related management and orchestration systems.

		• Strategic and operational-level war-games. • Solutions and tools to reflect gender, age and other societal perspectives in relation to cyber operations.
Cyberspace Intelligence, Reconnaissance, Surveillance (CyISR)	This refers to activities whereby intelligence is derived in or through cyberspace.	• Solutions and tools in support of CyISR processes and activities (with emphasis on fusion/integration of CyISR with CySA and CyC2 products and workflows). • Generation of operational-level adversarial (or red) picture in support of CySA/CyC2, using Open-Source Intelligence (OSINT), Cyber Threat Intelligence (CTI) and other sources of information. • AI solutions and 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 out of scope*).
Offensive Cyber Operations (OCO)	This refers to activities in or through cyberspace that project power to create effects which achieve military objectives.	• OCO and cyber effects (direct and indirect) development and integration into joint targeting. • Operational risk analysis. • De-confliction mechanisms. • Battle Damage Assessment (BDA). • Cyber Identity Army concepts/tools – i.e., cyber identity armies implement the concept of cyber persona at scale and are made up of multiple classes of specialized (cyber) soldiers specialized that can undertake unique policies, tasks, rules of engagement, metrics for assessment, etc.

		• Integrating/Coordinating/Deconflicting Sovereign Cyber Effects provided voluntarily by Allies (SCEPVA) during planning prior to, and during operations • AI solutions and 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.	• Civilian-military integration. • Cyber integration into joint- and multi/cross/all-domain operations. • Integration/coordination of cyberspace operations with EMO, IO/cognitive warfare, or space operations. • Integration/coordination of cyberspace operations with • Cross-domain/cross command information sharing.

AI, 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. ➔ **HQ SACT is particularly interested in AI tools and solutions** that ultimately free cyberspace operators for more strategic tasks; this includes: ▪ Data correlation, prediction, prioritizations, and orchestrations. ▪ Process automation. ▪ Report generation and automation. ▪ AI-assisted rapid prototyping of cyber C2 systems. ➔ **HQ SACT will not provide large data sets of training data, but rather unclassified examples of cyberspace operations products (plans, reports, etc.)**. Proposed experiments which require these large training data sets will not be considered.	• AI-enabled ingestion, parsing and exploitation of free form, information sources in varied formats. • AI-enabled generation of information products, including reports, mission portals, RFI, operational pictures, etc. • AI-enabled CyC2 activities, including but not limited to development, analysis and management of CoA, planning, targeting and assessment. • AI Application Programming Interface (API) to interface Large Language Models (LLMs)/Retrieval Augmented Generation solutions with cyberspace capabilities such as CySAS, CyC2IS or the Threat Intelligence Analytics Platform (TIAP), among others. • Agentic AI solutions able to implement cyberspace operations workflows, automate processes, enhance data sources exploitation and support information development and dissemination. • AI-supported software development and rapid prototyping of CyC2 systems and tools, in support of CyC2 data, processes and outputs.

4.3. White Paper Format

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

a) **Short compliance statement**, confirming that the proposals comply with the RFI scope, meaning that they:
   a. Are not based on the demonstration of a commercial product.
   b. Are not cyber security focused.
   c. Contribute to (and support) cyberspace operations, from a military standpoint.
   d. Are affordable in terms of timeline and resources (see below ROM).
   e. Do not require large training datasets nor access to actual classified information.

b) **Experiment proposal(s)** formulated in terms of objectives, hypotheses, success criteria, technical set up, metrics, etc. Experiments should seek to provide a meaningful deliverable/product upon completion.

c) **Brief description** (maturity, use cases, etc.) of the concept, product or capability to be experimented with.

d) **Effort/cost (ROM[5])** required to conduct the proposed experiment.
   ➔ *To help guide respondents, HQ SACT wishes to highlight that first-phase experiments are usually **modest in scale**, often completed within about **six months** and designed to operate within a **limited level of effort**.*

e) **Other relevant information**, including constraints or limitations related to the experiment proposal.

f) **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. 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.

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

4.3.3. 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).

4.3.4. 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>.

[5] 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.

4.3.5. 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.

4.4.6. 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.

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

4.6.8. 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 may invite a selected number of RFI respondents to present their proposal and engage with the NATO/Allies operational community during a cyberspace warfare development and experimentation workshop. This event may take place in Q2 2026 (TBC).

4.4. Response Due Date. Responses to this RFI must be received by **9:00 an EST 20 March 2026**. The responses shall not contain any classified information. HQ SACT reserves the right to seek clarification on submissions. HQ SACT will notify all companies upon completion of the assessment of the proposals, which might take several weeks.

5. CLARIFICATIONS AND QUESTIONS

5.1. All questions should be submitted by e-mail solely to the aforementioned POCs by **9:00 am EST 27 February, 2026** to allow for appropriate response time prior to the **9:00 am EST 20 March 2026** 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 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 Request for Information (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 an RFI, and not an Request for Proposals (RFP) of any kind.

***