RFI: **RFI-ACT-SACT-26-26-Cyberspace Warfare Development and Experimentation Campaign**

Reference: Q&A #1

Date of Issue: 03/9/2026

The following questions were raised with respect to subject **RFI-ACT-SACT-26-26-Cyberspace Warfare Development and Experimentation Campaign.** Responses are to provide clarification.

Questions	Responses
1. What role does NATO envision for the solution provider within the experiment (e.g., red team, blue team, provider, observer, or other)?	As a reminder, this Request for Information aims to collect experiment proposals related to existing and under-development cyberspace operations concepts, products or capabilities at military/mission-level. RFI respondents are free to propose the set-up, including roles, that they think would best support their proposed experiment objectives and hypotheses.
2. What level of technical depth is expected (e.g., tabletop discussion, hands-on keyboard execution, integrated live exercise, or another format)?	Experiments can leverage many techniques and constructs (tabletop, wargame, etc.) to validate concepts, elicit requirements or explore groundbreaking technologies. ACT is open to all options, provided that the proposal is feasible (see next question). At this stage, only a brief description of the proposed experiment is expected, as per paragraph 4.3.1 of the RFI document.
3. Based on your 2024 CySA experimentation campaign, what key elements were particularly successful and should be considered or built upon?	Experiment proposals shall be feasible in terms of scope, resources, and timeline. They shall be based upon available data (not classified, no large training datasets required, etc.). They shall clearly identify inputs, processes, and outputs to allow ACT to assess feasibility.
4. When referring to a “crisis exercise” versus a “cyber range,” is NATO distinguishing between simulation-based decision-making exercises and hands-on technical execution environments?	Cyber Ranges are the platforms/capabilities that allow for the simulation and implementation of use cases, processes, and tools. The “crisis” aspect rather refers to the scenario being used for a specific exercise, utilizing, as needed, a Cyber Range. Both are not mutually exclusive. While ACT is interested in ETE solutions, including Cyber Range tools, in support of cyber force training, pure technical level exercise solutions (e.g., at network defender level) is not in scope.
5. Is a US-incorporated LLC (chartered in South Carolina) is eligible to respond under Section 4.4.6 without requiring a NATO nation partner, since the US is a NATO member nation. Keep it to 3-4 sentences. Ask if there are any	US LLC’s are eligible to respond to an RFI as the US is a member nation.

additional eligibility requirements for US small businesses responding to HQ SACT RFIs	
6. The NATO RFI states the customer is interested in experimental capabilities that may include industry's existing or planned concepts, products, or capabilities. These concepts, products, or capabilities are often developed by contractors at their own expense and descriptions of these capabilities and capability prices are proprietary. The NATO RFI states that all submissions must be unclassified and non-proprietary. Can NATO provide a method of delivering white papers that contain either NATO classified information or contractor proprietary information?	As indicated in the RFI instruction document, responses shall not contain classified information and as a recommendation, shall not include proprietary information. To comply with this requirement, high level description of concepts, products, and capabilities, without comprehensive technical description and pricing, is acceptable at this stage. As per paragraph 6.3, proprietary information, if there is any, should be clearly marked and will be treated 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.
7. The NATO RFI states that selected RFI members may be invited to present their work at a NATO workshop in Q2 2026. Many of the cyber capabilities contractors could submit benefit from being unpublished. Both a public workshop presentation and wide distribution of RFI responses describing these capabilities could seriously reduce the value of the capabilities contained in the white paper. Can NATO provide a method of delivering white papers with restricted distribution to only the HQ SACT office?	Please refer to paragraph 6.1 for Non-disclosure Principles and/or Non-disclosure Agreement (NDA) with Third Party Company. As a general rule, RFI responses are not widely shared and are mainly kept within HQ SACT to inform cyberspace warfare and capability development activities. Industry may be invited to brief their proposal at a dedicated workshop, which is not public and only include representatives from NATO organizations and Nations. These briefs are completely optional and declining to provide them will not be detrimental for the proposals.
8. The NATO RFI states that proposed concepts must meet NATO policy, doctrine, or requirements in cyberspace operations. Can NATO provide copies of or reference number for the NATO policy, doctrine, or requirements for offensive cyber operations?	RFI respondents shall refer to publicly available information related to NATO cyberspace doctrine and policy – for instance AJP 3.20 (available here) and NATO HQ cyber defence resources (available here). Link 1 https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf Link 2 https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence
9. The NATO RFI states that responses should be accompanied by a non-binding ROM. In the ROM description NATO askes for the cost of first phase experiments. Earlier in the NATO RFI	The ROM shall cover the costs to conduct the proposed experiment in support of ACT's cyberspace warfare development efforts (e.g., engineering support, experimentation documents, project management). Minimal

requirements mentioned NATO's desire for prototypes. Can NATO clarify what level of function / capability should be priced in the ROM?	development – beyond the limited tailoring to the experiment needs – is expected for such effort as the idea is to leverage and test an existing concept/capability. The cost should be commensurate with the development of a self-contained experimentation product by end of 2026 (i.e., multi-year developments, unless they deliver a clear self-contained product per year, shall in general not be considered).
10. The NATO RFI states that responses should be accompanied by a non-binding ROM. Can NATO clarify if the price should include an anticipated cost for the data rights of the capability? If yes, what level of data rights would NATO require?	The ROM is expected to include all the anticipated costs to conduct and support the proposed experiment. HQ SACT expects to obtain ownership over data generated from the experiment.
11. Are we required to have prior experience in military projects to participate?	While prior military project experience may help tailor your inputs, this is not a requirement to respond, as long as the proposal is within the RFI scope.
12. Could you please provide more precise ROM (Rough Order of Magnitude) budget values? The information about a 6-month experiment duration does not clarify the expected costs (e.g., AI tokens, personnel, infrastructure, etc.).	The ROM shall cover the costs to conduct the proposed experiment in support of ACT's cyberspace warfare development efforts (e.g., engineering support, infrastructure, experimentation documents, project management). Minimal development – beyond the limited tailoring to the experiment needs – is expected for such effort as the idea is to leverage and test an existing concept/capability. The cost should be commensurate with the development of a self-contained experimentation product by end of 2026 (i.e., multi-year developments, unless they deliver a clear self-contained product per year, shall in general not be considered).
13. Should the experiments include a Proof of Concept (PoC) as part of the scope?	Depending on the concept/capability maturity, the proposal can be articulated around a Proof of Concept to demonstrate feasibility.
14. Should the white paper contain a detailed description and/or a plan for developing a Proof of Concept?	If the proposal relates to a Proof of Concept, the white paper shall contain a description in terms of objectives, hypotheses, success criteria, technical set up, maturity, use case, etc., as stated in paragraph 4.3.1.
15. Are there any limitations regarding the number of white papers that can be submitted per domain and/or per submitting organization?	No, again provided that the white papers are within the RFI scope.
16. What is the required information classification level at this stage (e.g., "Unrestricted" information only)? Additionally, will these requirements	Responses to this RFI shall not be classified above NATO Unclassified and shall not contain proprietary information. As a reminder, this is a Request for Information (RFI) only and does not constitute a commitment to issue a future

change at later stages such as RFI or RFQ?	Request for Proposal (RFP). Classification requirements regarding potential future stages will be specified in due course, as needed.
17. Would the Government consider allowing a CUI response to RFI-ACT-SACT-26-26?	As indicated in the RFI instruction document, responses shall not contain classified information and as a recommendation, shall not include proprietary information. To comply with this requirement, high level description of concepts, products, and capabilities, without comprehensive technical description and pricing, is acceptable at this stage. As per paragraph 6.3, proprietary information, if there is any, should be clearly marked and will be treated 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.
18. Are export controlled responses acceptable, and if so, are there special handling procedures we will need to use?	Responses to this RFI shall not be classified above NATO Unclassified and shall not contain proprietary information. As a reminder, this is a Request for Information (RFI) only and does not constitute a commitment to issue a future.
19. Is an experiment tailored for NATO, but based upon an existing platform acceptable?	Yes, the idea for experimentation effort is to leverage/reuse existing concepts, capabilities and tools to limit additional development activities.
20. What maturity level does NATO expect for a “tangible deliverable”?	When mentioning tangible products/deliverables, ACT refers to activities/experiments leading to the development and validation of a concrete product, which can be a prototype, tool, concept, etc. Tangible products/deliverables are expected as part of this effort, as opposed to sole demonstration. While a high level of maturity is preferred, it will not be the main selection criteria
21. Please clarify what qualifies as meaningful success criteria and metrics.	Experiment success criteria and metrics are expected to be defined in the experiment proposal. They can include qualitative and quantitative elements. In general terms, experiment success will be measured against product delivered, concept validated, etc. and will mainly look at usefulness to resolve an operational problem or need.
22. What constitutes “large amounts of training data”? What data availability constraints exist for AI experimentation?	Large amounts of training data are often required to develop and implement AI use cases. Due to classification/constraints, ACT would only be able to provide notional and limited data (for instance one or two synthetic OPLANs, one mission scenario, a few sets of cybersecurity incidents, etc.). Such constraints and limitations should be kept in mind when developing AI related proposals.

23. What are integration expectations with CySAS / CyC2IS / TIAP?	While integration is required between NATO cyberspace capabilities (CySAS, CyC2, TIAP, etc.), constraints and limitations will most likely not allow for such activities as part of an experimentation effort. Possible automated integration/exchange of information between the proposed experiment and existing/under development capabilities can be highlighted, but they are not expected as part of 2026 efforts.
24. How strictly does NATO interpret the operational vs. technical boundary?	Please refer to RFI scope. While both levels are closely interrelated, operational level activities are understood as workflows and processes supporting mission/military level activities (planning, executions, assessment, etc.), aimed at guaranteeing mission assurance. Technical level activities are those conducted by asset managers and service providers to guarantee information assurance.
25. Please quantify “limited level of effort”. Are there any ROM and/or scale expectations for a 6-month first-phase experiment?	The ROM shall cover the costs to conduct the proposed experiment in support of ACT’s cyberspace warfare development efforts. It is expected to include engineering support, infrastructure, deployment support, experimentation documents, project management. Minimal development – beyond the limited tailoring to the experiment needs – is expected for such effort as the idea is to leverage and test an existing concept/MVP/capability. The cost should be commensurate with the latter requirements and with the development of a self-contained experimentation product by end of 2026 (i.e., multi-year developments, unless they deliver a clear self-contained product per year, shall in general not be considered).
26. What selection criteria will be used to evaluate engagement?	ACT will evaluate proposals based on operational relevance, usefulness of the concept/capability/tool, level of maturity and feasibility (as per RFI scope). Follow-on engagements will be envisaged, as needed, to seek clarification and/or consider potential next steps. As a reminder, this is an RFI, not linked to any particular RFP/RFQ.
27. In the context of experimentation under NATO UNCLASSIFIED conditions, would representative tactical communication scenarios with emulated bandwidth and latency constraints (e.g. SATCOM-like conditions) be considered acceptable for validating post-quantum migration feasibility, provided no	Please note that, in general, transmission/transport, communications and core services are considered part of technical service provisioning and, therefore, of interest for service delivery and cyber security. If no clear linkage with operations, mission, and tasks/activities is found, this might not be of interest for ACT.

operational networks or classified data are involved?	
28. For experimentation involving representative commercial embedded platforms (e.g. FPGA/SoC development boards), would structured resilience assessment under controlled laboratory conditions be considered within scope, provided the objective is to derive mission-level resilience indicators rather than to conduct vulnerability testing?	In general, cyber resilience is not part of the area of interest of the RFI. Formal/quantitative/procedural evaluation of mission assurance based on cyber service health and status would be within the area of interest, as it would be the courses of action development and assessment to prioritize service-level cyber security efforts to enhance mission assurance.
29. From an operational perspective, which categories of mission-level metrics would HQ SACT consider most valuable for experimentation in post-quantum migration scenarios (e.g. communication availability, decision latency impact, interoperability stability, resilience classification thresholds)?	Please note that, in general, transmission/transport, communications and core services are considered part of technical service provisioning and, therefore, of interest for service delivery and cyber security.
30. How critical is attribution resistance for OCO effectiveness?	This type of details/assumptions will be discussed should a company be selected to deliver a product/solution for NATO operations.
31. What latency/performance requirements exist for cyber operations? Is distributed execution acceptable?	Distributed execution is a valid assumption. Latency/performance requirements can be discussed should a company be selected to deliver a product/solution for NATO operations
32. What types of operations would benefit most from distributed execution? (OCO, DCO, CyISR?)	This type of details/assumptions will be discussed should a company be selected to deliver a product/solution for NATO operations.
33. Do operational planning assumptions or informal performance requirements exist for cyberspace task execution in degraded scenarios—across DCO, OCO, and CyISR— or is defining those thresholds expected to be part of the experimental output?	This type of details/assumptions will be discussed should a company be selected to deliver a product/solution for NATO operations
34. Are there specific task categories where HQ SACT would explicitly accept slower execution (e.g., 80–250ms overhead) in exchange for infrastructure resilience and operational continuity?	The companies responding to the RFI shall identify the most plausible working assumptions.
35. Is there an existing NATO legal or policy basis for civilian compute providers participating in operationally-adjacent infrastructure under NATO command authority, or is this genuinely novel territory?	NATO policy assumes participation of civilian elements and organizations in cyber operations. Companies responding to the RFI are free to specify models for integrating civilian components, which night inform future policy development if they are found relevant and feasible.

36. What eligibility or vetting criteria (e.g., NATO-nation incorporation, security screening, audit obligations) would HQ SACT consider minimum necessary for civilian node participation?	Respondents are free to determine models of engagement (form information sharing to operational activities) which can be further analyzed in terms of policy, legal frameworks, feasibility and usefulness/contribution to commander's objectives.
37. Has civilian commercial infrastructure been integrated into operational execution environments in any previous NATO exercises, including Cyber Coalition?	Yes
38. What are the primary deconfliction failure modes HQ SACT is most concerned about in SCEPVA scenarios: temporal conflict, geographic conflict, authority-level conflict, or something else?	These detailed considerations exceed the level of classification of the RFI.
39. Does an existing CyC2IS data model, API specification, or deconfliction schema exist that an experiment should align with, even if only in unclassified representative form?	These detailed considerations exceed the level of classification of the RFI.
40. Do NATO Allies conducting joint cyberspace operations rely on shared or interdependent communications and coordination infrastructure, or does each Ally maintain operationally self-contained capability?	This type of details/assumptions will be discussed should a company be selected to deliver a product/solution for NATO operations.
41. If one Ally's CyC2IS infrastructure is degraded, to what degree does that affect the operational continuity of other Allies in the same theatre?	This type of details/assumptions will be discussed should a company be selected to deliver a product/solution for NATO operations.
42. Is cross-Ally infrastructure fallback—operating through another Ally's coordination nodes—an established practice or a gap that DCOEP should factor into its design?	This type of details/assumptions will be discussed should a company be selected to deliver a product/solution for NATO operations.
43. Does HQ SACT have predefined experimental boundaries regarding the autonomous execution of Defensive Cyberspace Operations (DCO) when Human-in-the-Loop (HITL) communication is technically severed?	This type of details/assumptions will be discussed should a company be selected to deliver a product/solution for NATO operations.
44. Will the experimental framework provide simulated Rules of Engagement (RoE) specifying the threshold for delegated automated failover versus tasks requiring positive human confirmation?	Yes, if needed.
45. Does HQ SACT envision any scenario where pre-authorised, rule-based delegation of execution authority	This type of details/assumptions will be discussed should a company be selected to deliver a product/solution for NATO operations.

between Allies would be doctrinally acceptable during degraded connectivity?	
46. Beyond technical execution logs, does HQ SACT expect traceability of decision rationale in multi-Allied coordination scenarios, including prioritisation or suppression of sovereign effect requests?	This type of details/assumptions will be discussed should a company be selected to deliver a product/solution for NATO operations.
47. Would the inclusion of structured "decision-layer" audit artefacts—separate from execution telemetry—be considered value-added within the experimental scope?	Audit is an essential part of cyber C2.
48. We will propose a complete solution to ensure verification of information coming from different sources. Is there any existing system to add and improve on so we can propose a complete solution from a to z to address and resolve this issue?	The proposed solution should not be dependent on availability and use of other capabilities.
49. Non-alignment of intelligence info coming from different sources. We are in condition to propose a complete verificable system that can resolve this. Is it of NATO interest to get a proposal in this specific matter?	Yes
50. Has NATO formally identified a need for more systematic intelligence verification through a requirements process, exercises, or operational experience?	Yes
51. Has NATO identified adversarial intelligence manipulation—injecting or modifying objects before they reach CySAS or CyC2IS—as an active threat?	This information exceeds the level of classification of this exchange.
52. Traceability log for updates/modifications to intelligence information. Would it be of interest to NATO that we offer a traceability system to scale and enhance data input for decision making models?	Yes
53. We are in condition to deliver a solution to identify if intelligence data was a factor to failure of cyberspace operations or when they generated wrong outputs. Is this of interest?	Yes
54. Would multi-source validation help detect manipulated intelligence?	That should be answered by the proposed response to the RFI.
55. How fast does intelligence need to move from collection to CySA exploitation?	Respondent is expected describe the proposed solutions, including expected performances.

(e.g., is a 200–800ms ledger confirmation delay acceptable for operational loops?)	
56. CySAS Integration: What data ingestion standards/APIs does CySAS support? Would intelligence verification metadata enhance CySAS decision support?	This type of details/assumptions will be discussed should a company be selected to deliver a product/solution for NATO operations.
57. CyC2IS Workflow: How do current CyC2 processes handle intelligence confidence levels when generating Course of Action (CoA) recommendations?	This type of details/assumptions will be discussed should a company be selected to deliver a product/solution for NATO operations.
58. TIAP Compatibility: Does TIAP currently distinguish between verified and unverified intelligence?	This information exceeds the level of classification of this exchange.
59. Does HQ SACT operate with an endorsed or emerging operational-level ontology that governs data exchange across CySAS, CyC2IS, and TIAP?	Respondent shall describe a potential solution/product including all necessary assumptions about ingested data and supporting artifacts like ontologies.
60. In cases of divergent adversarial pictures, is there a formalized doctrinal/technical resolution mechanism, or does reconciliation remain staff driven?	Respondent shall describe a potential solution/product. Mechanisms to adapt it to NATO shall be part of conversations with a company selected to deliver a product/solution for NATO operations.
61. Is there interest in quantifying intelligence contributions for burden-sharing assessments?	Yes
62. Is it of interest to have a hierarchy of data credibility depending on the national member that sent the info?	No. It should if “national member” was replaced by “data source”
63. Is it of interest to have a proposal about sharing intelligence by different members of the nato alliance?	Please make your best assessment if in line with the scope of the RFI and submit if necessary.
64. Does NATO currently apply any reliability weighting to intelligence specifically based on the contributing nation?	This information exceeds the level of classification of this exchange
65. Are there active policy discussions around structured multi-national CyISR intelligence sharing that this experiment could feed into?	This type of details/assumptions will be discussed should a company be selected to deliver a product/solution for NATO operations
66. Would NATO provide sample (unclassified) intelligence reports for prototype development, or must we generate synthetic test data?	Both options are possible. NATO could provide a handful of representative examples, which might or not be synthetic.
67. Could an intelligence verification prototype be tested during NATO's Cyber Coalition exercise (2026 or 2027)?	It depends on the technical feasibility, but more importantly on the relevance and the interest for the operational community.

68. What is the specific process and required lead time for proposing integration into the Cyber Coalition 2026 or 2027 exercises?	Exercise execution takes place during the last week of November or first week of December. The experiment does not necessarily need to adapt to the exercise planning events.
69. Is data normalization (fixing formatting, removing duplicates, standardizing nomenclature) an expected function of a system integrating into CySAS and TIAP?	This information exceeds the level of classification of this exchange
70. Would it be a requirement to cleanse data received from NATO data sources?	Respondent should explain the purpose of the product/solution/tool to experiment, including all necessary working assumptions.
71. What is the time criticality for intelligence transmission and validation? How fast must intelligence be verified and disseminated?	This information exceeds the level of classification of this exchange
72. Do AI-driven decision support systems require higher intelligence quality/verification levels than human analysts?	Yes. This is a universal truth.
73. Would automated systems benefit from machine-readable verification metadata?	Yes. This is a universal truth.
74. Is there an existing or emerging NATO standard for machine-readable intelligence verification metadata (source type, confidence, history) that AI tools consume?	Respondent should not make any assumption about this, at this point, as such standards are not expected to be integrated into 2026 efforts.
75. The RFI states that proposals to "demonstrate a commercial product" will not be considered. Can HQ SACT clarify the distinction between demonstrating a commercial product and adapting/experimenting with a mature commercial technology in a novel NATO operational context?	Leveraging an existing/commercial product is fine providing that it is based on an articulated experiment proposal aimed at validating concepts, use cases, etc. (as stated in 4.3.1).
76. Can HQ SACT confirm that a Canadian-headquartered company with no existing NATO contracting relationship is eligible to respond and participate in follow-on experimentation activities?	Yes, industry that originated within a NATO country is eligible to respond
77. The RFI distinguishes between "technical/network-level" activities (out of scope) and "mission/operational-level" activities (in scope). Can HQ SACT provide further guidance on where network infrastructure orchestration and monitoring falls, specifically, when network-layer visibility is used to inform mission-level CySA and CyC2 decision-making?	Network monitoring is considered to be at technical-level, managed by the service provider. It can be considered within the RFI scope provided that the connection to operational/mission level activities is done (for instance in terms of impact to mission tasks and activities to evaluate mission assurance). It needs to be noted that, in general, proposals covering technical capabilities and tools will not be further

	considered unless a strong case to quantitatively impact operational activities is demonstrated.
78. The RFI references integration with CySAS, CyC2IS, and TIAP. Can HQ SACT confirm whether representative interface documentation, data schemas, or API stubs for these systems would be made available to selected experiment participants to support integration work?	While integration is required between NATO cyberspace capabilities (CySAS, CyC2, TIAP, etc.), constraints and limitations will most likely not allow for such activities as part of an experimentation effort. Possible integration/exchange of information between the proposed experiment and existing/under development capabilities can be highlighted, but integration during the experimentation campaign is not expected. Further information may be provided as part of follow-on efforts, as needed.
79. Are synthetic or notional NATO network topologies available for use in experiment environments, or is the respondent expected to generate their own representative scenarios entirely?	RFI respondent as free to generate their own proposal, as the supporting network/deployment model for experiments are not defined at this time, and as described in the RFI the underlying technical layer (networks and services) are not the in the main scope of the RFI.
80. The RFI states experiments should deliver a "tangible product (demonstrator, minimum viable product, concept, etc.)." Can HQ SACT confirm that a software-based working demonstrator deployable in a lab environment meets this requirement?	Yes. When mentioning tangible products/deliverables, ACT refers to activities/experiments leading to the development and validation of a concrete product, which can be a prototype, tool, concept, etc. Tangible products/deliverables are expected as part of this effort, as opposed to sole demonstration.
81. What is the anticipated level of NATO/Allied operator involvement during the demonstration and evaluation phase — will HQ SACT provide evaluators, or is the respondent expected to recruit participating personnel?	Depending on the experiment scope and needs, ACT will bring representatives from NATO/Allied operational community.
82. The RFI mentions a potential Q2 2026 workshop where selected respondents may present. If selected, would travel and presentation costs associated with attending the workshop be covered by HQ SACT or borne by the respondent?	If confirmed, industry briefs to this event will be conducted via VTC.
83. The RFI mentions that HQ SACT "may explore the possibility of allocating limited funding" to support selected ideas. Can HQ SACT provide any further guidance on the scale, mechanism, or timeline of any such funding allocation to help respondents plan appropriately?	This clause applies only to this RFI submission. For information, ACT General Terms and Conditions are available on ACT website: https://www.act.nato.int/wp-content/uploads/2026/01/HQ-SACT-General-Terms-and-Conditions-20260115.pdf
84. If HQ SACT contracts a third party to review submissions under NDA, will respondents be notified of the identity of that third party prior to their submission being shared?	In principle, submissions review will be performed by ACT staff.