RFI:

RFI-ACT-SACT-25-22-Cyberspace Warfare

Reference:

Q&A #1

Date of Issue:

18 March 2025

The following questions were raised with respect to subject **RFI-ACT-SACT-25-22-Cyberspace Warfare.** Responses are to provide clarification.

Questions	Responses
1. Are there any limits to the use of digital twins and their magnitude?	No limits
2. Would the scenarios have to use fictitious countries?	For the purpose of this RFI, any proposed solutions/concepts should be agnostic to this aspect. Scenarios are confirmed during the implementation phase, in line with NATO applicable policies and security domains, generally keeping the scenario at unclassified level. If the organization prefers to use a different scenario, then it will need to be unclassified, with no limitations to sharing, and approved by HQ SACT. The scenario shall not make references to real nations/forces.
3. How would the Cyber Range Digital Library be regulated and controlled among different NATO member states?	NATO cyber range digital library is part of the NATO cyber range capability, and therefore available to all NATO nations during NATO use of the cyber range. All administrative activities are dealt with between HQ SACT and the cyber range organization.
4. Can you please provide additional information about the experimentation test environment?	The experimentation test environment is not defined at this stage. HQ SACT conducted in the past several experiments using NATO Unclassified Cyber Range (NUCR) in Tallinn, Estonia, but other technical set-ups (e.g., cloud-based) can be envisaged, as needed. RFI respondents shall not be constrained by this aspect.
5. Will the experimentation test environment replicate the current NATO tactical communications network?	Depending on the experimentation hypotheses and objectives, many technical setups can be envisaged, the replication of NATO (mission) networks being only one of them. RFI respondents shall not be constrained by this aspect. If the experiment requires emulation of NATO networks, then the test environment should replicate NATO strategic and operational networks, and/or national tactical networks. Please note that in general, network emulations are used for cyber security experiments, which are out of the scope of this

	RFI. The majority of operational-level capabilities experiments do not require extensive network emulation.
6. Will the experimentation environment include white(friendly), gray(neutral), and red(enemy) cyberspace?	The experiment proposal should determine this. Depending on the experimentation hypotheses and objectives, all the cyberspace (or only portion of it) can be emulated. RFI respondents shall not be constrained by this aspect. HQ SACT is open to any proposals, provided that they support operational/military level Use Cases.
7. Will the vendor be utilizing NATO forces to run through scenarios to test experiment objectives?	NATO missions/units may be emulated as part of the experiment scenario(s) in order to test and validate hypotheses. HQ SACT can also coordinate participation and involvement of NATO operational community (e.g. Allied Command Operations, Joint Force Commands) into the experiment, as necessary.
8. Will the vendor be responsible for funding all experimentation procurement and execution activities after response to this RFI and any follow-on RFPs? I didn't want to make assumptions based on the ROM requirement.	As indicated in the RFI within section 1.3, 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. This will include any responders that are invited to subsequent events. Any follow-on RFPs will be competed in accordance with NATO procurement regulations and will be made available on the HQ SACT website.
9. At which classification level will the experiment operate?	Generally, HQ SACT experiments are conducted in an unclassified environment.
10. Could an experiment like this [testing the robustness of virtualization using a formally verified hypervisor (seL4) in a Windows environment] be of interest to you? We are a small company, and we need to be very sure where we dedicate our resources (including preparing a proposal).	This RFI seeks concept and experiment proposals in the area of cyberspace operations. Cyber-security/CIS-security solutions are not in scope of this RFI. With limited knowledge on this topic, HQ SACT initially assesses that such experiment would rather belong to the realm of cyber security, but if Use Cases at the operational/military-level exist, industry partner is welcome to submit a proposal for review.
11. If it is of interest to you, what benefit would we gain as a company if our proposal is chosen? Could we publicize it?	As indicated in the RFI, industry providing proposals will have the opportunity to inform and shape NATO cyberspace warfare and capability development activities, which can result in potential collaboration opportunities (such as follow-on experiments or feasibility studies, funded by HQ SACT, and exposed to the wider NATO community). In general, companies participating in NATO cyber experiments can publish press releases and press notes after HQ SACT approval.