RFI: **RFI-ACT-SACT-23-16 - Cyberspace Wargame**

Reference: Q & A # 1

Date of Issue: 14 March 2023

The following questions were raised with respect to subject RFI. Responses are to provide clarification.

Questions	Responses
1.Is the RFI Cyber wargame outcome to be situated within a representative MDO relevant scenario with Cyber operations supporting all 5 domains?	1. The Cyber Wargame should be domain-specific. The wargame needs to focus on cyber-attacks that have a strategic and/or political impact on an Alliance, national and/or international level. Civilian and military cooperation in cyberspace should play a relevant role in the wargame.
2. What is the anticipated size of training audience and what is the expected Pol / MilStrat split?	2. At least 32 participants representing NATO Nations with one counsellor each are expected. The wargame should cover both areas at the same time. However, the focus is on the political level. Additionally, civilian and military representatives on several levels could to be included (NAC, MC, SACEUR, CyOC for mil and comparable institutions for civ).
3. Is it a distributed / virtual or a in-situ in person event?	3. Participation in person is possible. However, a distributed wargame, would be more appealing and might allow better participation and representation for all the different entities from above. Video conferencing facilities for classified content are available.
4. What is the number and duration of individual wargame events (including any development serials ahead of the main serial)?	4. The execution of the wargame should not take longer than one working day. For the final execution of the wargame, two iterations are expected. However, multiple test runs for the cyberspace wargame are expected to be executed within HQ SACT or other NATO entities. It is planned to use the Cyber Coalition Exercise Nov-Dec 2023 as a test run for a prototype of this cyberspace wargame, if development timeline allows.
5. What is the availability of NATO (NCS and CoE) personnel support to the Cyber SME LOCON?	5. Answer: SMEs from various NATO institutions would be invited to support.
6.What would be the preferred timeframe to run the first wargame?	6. The execution of the wargame should not take longer than one working day. It is planned to use the Cyber Coalition Exercise Nov-Dec 2023 as a test run for a prototype of this cyberspace wargame, if development timeline allows. The preferred timeframe for the final execution of the wargame, which has not been planned and scheduled yet, is Q3/Q4 2024.
7. What expected budget range for the wargame?	7. There is currently no specific budget. The respondents are expected to including their considerations about the design, development, execution, analysis and reporting of the cyberspace wargame to achieve the wargame objectives. When applicable, please provide a brief description of the effort/cost required to finalize its implementation/adaption/adoption.
8. If invited to participate in the conference in Lillehammer, would that travel be reimbursed?	8. The Participation at TIDE Sprint Conference can be both in person or remote, via VTC. Conference registration costs and travel are at participant expenses. A limited number of respondents will be offered to brief (technical, not corporate briefs are expected) on their solutions, based on the applicability of their responses to this RfI.
9. Will players have access to Virtual Reality equipment, or would the contractor be expected to provide such equipment if used?	9. The contractor would be expected to provide such equipment if used.
10. Will players have access to computers for use during the game, or would the contractor be expected to provide such equipment if used?	10. This depends on the technical solution. There is a trade-off between technology used and operational value. The wargame could be conducted on the NATO unclassified cyber range. If so is the case, NATO would provide the majority of the required workstations. The

	contractor would be expected to provide wargame software, any VR equipment (if necessary), and any additional hardware that is essential on top of standard NATO workstations and servers. However, this possibility could limit the operational value, as higher classified content could not be covered.
11. If Artificial intelligence is used for the game, would there be GPU processing capabilities available for calculations, or would the contractor be expected to provide such capabilities?	11. The contractor would be expected to provide such equipment if used.
12. Are the any data sources that the game can use, or which the game should use? (e.g. the wargaming team would have access to OR would be expected to use a specific database for vulnerabilities)	12. The contractor would be free to choose any data or threat scenarios as long as they are realistic and appropriate for the political level or military strategic level. The cyberspace wargame needs to focus on cyber-attacks that have a strategic and/or political impact on an Alliance, national and/or international level. The contractor will have access to relevant NATO policy, doctrine and TTPs. The contractor will not need access to other data sources, unless justified in the response and considered needed for the purposes of the wargame, and releasable in accordance with NATO security policies and regulations.
13. Would remote gameplay (if any) be over public internet or over government networks?	13. Participation in person is possible. However, a distributed wargame, would be more appealing and might allow better participation and representation for all the different entities. If designed in a distributed manner, the Wargame software shall preferably make use of NATO unclassified cyber range. Users could connect either in-place (CR14, Tallinn) using cyber range provided work stations, or remotely using (preferably) NATO unclassified workstations. Non-NATO workstations, VR sets, GPUs and other devices would preferably connect to NATO cyber range via VPN, from any internet accessible location.
14. Would any groups in NATO or supporting governments and militaries be available as role-players to support the wargame?	14. Yes, role players from various NATO institutions would be invited to participate.
15. How many iterations of the game are preferred?	15. For the final execution of the wargame, two iterations are expected. However, multiple test runs for the cyberspace wargame are expected to be executed within HQ SACT or other NATO entities. It is planned to use the Cyber Coalition Exercise Nov-Dec 2023 as a test run for a prototype of this cyberspace wargame, if development timeline allows.
16. How many participants are expected at a time?	16. At least 32 participants representing NATO Nations with one counsellor each are expected. Additionally, civilian and military representatives on several levels could to be included (NAC, MC, SACEUR, CyOC for mil and comparable institutions for civ).
17. Are there any special technological requirements expected for game provision? (e.g. any technology must legally run on government networks)	17. The preferred network and system is the NATO unclassified cyber range, which has very limited restrictions. Any other solution will have to be analysed on a case-by-case basis.
18. Where will the games be played? (e.g. in the offices where people work, in a special location)	18.The venue has yet to be explicitly determined, and it will depend on the wargame design. The network availability and the ability to use network and resources in a NATO security policies compliant manner indicates that the design should preferably be done using the NATO cyber range resources.
19. Which languages should game play use?	19. Answer: English (UK)
20. Would players be only from NATO member states, or would they include players from other countries?	20. The players would be only from NATO member states. Please note that Finland and Sweden will be invited by default.
21. Will it be possible to include equipment purchases (or rental) if participants do not have necessary equipment?	21. It would be. However, please note the complexity of connecting external HW/SW to NATO classified networks.
22. If a contract were offered, is it expected to be a single year contract or a multiyear contract?	22. This is only a RFI and does not constitute a commitment to issue a future Request for Proposal (RFP) or a subsequent contract.

23. Would each iteration of the game constitute its own contract, or be part of a single contract?	23. This is only a RFI and does not constitute a commitment to issue a future Request for Proposal (RFP) or a subsequent contract.
24. Would any contract include travel, or is travel expected to be billed separately?	24. This is only a RFI and does not constitute a commitment to issue a future Request for Proposal (RFP) or a subsequent contract.
25. How would the contract be paid? (e.g. upon delivery, half up front)	25. This is only a RFI and does not constitute a commitment to issue a future Request for Proposal (RFP) or a subsequent contract.
26.If invited to participate in the conference in Lillehammer, would that travel be reimbursed?	26. The Participation at TIDE Sprint Conference can be both in person or remote, via VTC. Conference registration costs and travel are at participant expenses. A limited number of respondents will be offered to brief (technical, not corporate briefs are expected) on their solutions, based on the applicability of their responses to this RfI.