EUROPEAN DEFENCE AGENCY

COMMUNICATION

EDA202107036/CAP/ISU/DA 22 July 2021

EDA documentation for Government use only

Martin KONERTZ
Director Capability, Armament and Planning
CAP@eda.europa.eu
T. +32 2 504 28 50

To: pMS' NATIONAL DEFENCE INDUSTRY ASSOCIATIONS (NDIAs), AEROSPACE AND DEFENCE INDUSTRIES ASSOCIATION OF EUROPE (ASD)

Copy: Central PoCs, Brussels PoCs, CAP PoCs and NAD PoCs

INDUSTRY ENGAGEMENT ON THE 1ST EDA WORKSHOP ON CYBER AND ELECTROMAGNETIC ACTIVITIES – CALL FOR PAPERS

Annex: EDA CEMA Workshop – Abstract template

Context

Cyber and ElectroMagnetic Activities (CEMA) are key enablers for operational success in the defence area and will determine the defence policy of subsequent years. To explore state of the art and assess innovation readiness, current technologies, and solutions supporting the CEMA convergence, the EDA intends to gather virtually the European key stakeholders from participating Member States (pMS). In organising the workshop EDA is supported by a contracted Consortium consisting of GMV, CINAMIL and Vedette.

For the scope and purpose of this call, convergence is defined as getting security/risk management functions to work together seamlessly, closing the gaps and vulnerabilities that exist in the space between functions to achieve operational superiority. Fully converged functions are generally unified and interconnected, reporting to one security leader. They often have shared practices and processes, as well as shared responsibility for security strategy. Converged functions work together to provide an integrated defence.

The purpose of the 1st EDA Workshop on CEMA is, (1) to derive insights about the convergence of electromagnetic warfare (EMW) and cyber defence, (2) to assess the current technological and

innovation readiness, (3) to provide relevant benchmarks to compare strategies, plans, and operations, and (4) to determine best practices for creating more effective and cost-efficient security and risk operations. The virtual workshop will help to identify specific risks, threats, challenges, needs and technologies.

The CEMA Virtual Workshop 2021 aims to outline harmonised policies and practices in technology transfer, research and development, supply chain, communications, and information technology infrastructure security, providing the state of play of EU Member States in this area.

The workshop will explore, inter alia, the development of synchronisation and the coordination of CEMA activities/operations supporting the Common Security and Defence Policy Crisis Management Operation (CSDP CMO) Commanders.

In particular, the participants are invited to briefly address the following topics:

- What is the current state of play in the convergence of CEMA?
- What are the emerging technologies, threats and practices that will shape CEMA convergence?
- What are the primary sources of risk that you have identified in the CEMA Convergence?
- How to strengthen the cooperation among pMS (i.e., MoDs) and between them and the industry?
- What are the impacts for the Armed Forces, e.g., in training, doctrine, operations or support?
- Do you have any remarks/suggestions about the CEMA supply chain or envisage any risks?

Scope

The European Defence Agency, in collaboration with the Consortium, is promoting a workshop focused on the integration of Cyber and Electromagnetic Activities and is asking representatives from (Inter)governmental bodies or agencies (e.g., Ministries of Defence, Armed Forces, research centres, etc.) and relevant industries[1] to contribute to the discussion. Responses from academia, national research centres, and practitioners, experts and policymakers will also be considered. Depending on the response, the event will be scheduled with panel discussions and individual keynotes. Participation slots will be assigned based on the assessment of contributions and availability.

[1] The workshop is open to entities established in EU Member States without any limitations in terms of intellectual property rights, security of supply, security of information or export controls stemming from outside the EU. It is also open to entities meeting these criteria from countries having an Administrative Arrangement (AA) with EDA which are involved in EDA R&T activities. EDA will validate registration on a case-by-case basis according to the above approach, in line with EDA's industry engagement policy.

Attendants are requested to provide an abstract of no more than **1000 words along with short biographical note(s) of the author(s) (100-150 words), including contacts and affiliation (use this template to submit your proposal)**. The abstract could focus on one or more of the topics/questions and provide assessments such as specific security challenges based on the contributor's experience, focus on technology evolution of solutions, detailed product roadmaps, use cases or scenarios. The submission of an abstract is not mandatory to governmental participants.

The abstract, which should not contain commercially sensitive information, will determine the final invitations to the event and be handled respecting proper attribution. Submitters should also specify whether they have any limitation in presenting their views in a panel format, together with other industry partners.

The abstract, which must be submitted and presented in English, should indicate the purpose/significance, the methods, the findings, and the conclusions. The reviewing process does not address grammatical errors. Selected participants will have 10'/15' for oral presentation (with or without slides).

The proposals (oral presentation or abstract, using the template in Annex), clearly linking answers to questions, should be submitted to EDA by email to the EDA Programme Manager Cyber Defence, Mr. David Antunes (David.Antunes@eda.europa.eu) and copy to Prof. José Borges (jose.borges@academiamilitar.pt) and Mr. Marco Marsili (info@marcomarsili.it). Please, indicate a point of contact to coordinate possible participation in the workshop; any inquiries may be addressed by email to the same mailboxes.

Selection criteria

The event organisers will strive to select a broad spectrum of representatives to ensure a fair, objective and balanced discussion. Officers, researchers, scholars, experts, and practitioners are invited to submit their proposals in theoretical perspectives, case studies, or state-of-the-art extended abstracts.

The Organising Committee will assess the abstracts across the following criteria: industrial readiness; innovation and originality; a holistic approach, i.e., how different aspects are integrated and articulated with each other; ability to provide a broad overview in the context of electromagnetic and information-related fields, such as cyber defence and relation between the cyber domain and other military domains (multi-domain of operations).

EUROPEAN DEFENCE AGENCY

COMMUNICATION

Outcome

The abstract accepted will be published in a digital edited book with the proceedings of the CEMA Virtual Workshop 2021. The book will include the workshop program, figures, key findings, conclusions, and recommendations.

Timeline

- Abstract submission deadline: 26 August 2021
- Workshop execution: 14 September 2021. 14h00-18h00 (CET, GMT/UCT -1)

Martin KONERTZ