European framework and proofs-of-concept for the intelliGent aUtomAtion of cybeR Defence Incident mAnagemeNt

Marta Irene García Cid[1], Manuel Gil Pérez[2], José María Jorquera Valero[2], Antonio López Martínez[2], Jorge Maestre Vidal[1], Gregorio Martínez Pérez [2], Laura Méndez García[1], Frida Muñoz Plaza[1], Pantaleone Nespoli[2], Javier Pastor Galindo[2], Pedro José Ramón y Cajal Ramo[1], Francisco Antonio Rodríguez López[1*], Pedro Miguel Sánchez Sánchez[2], and Marco Antonio Sotelo Monge[1]

[1]Indra Digital Labs, Av. de Bruselas, 35, 28108 Alcobendas, Spain
Email: {migarcia, jmaestre, lmendezg, fmplaza, pjramon, farodriguez, masotelo}@indra.es

[2]*Department of Information and Communications Engineering, University of Murcia*, 30100, Murcia, Spain.
Email: {mgilperez, josemaria.jorquera, antonio.lopez41, gregorio, pantaleone.nespoli, javierpg, pedromiguel.sanchez}@um.es

***Abstract*—Artificial Intelligence and Automation are revolutionizing cyber defence and incident response by addressing traditional inefficiencies and enabling faster and easier incident resolutions. However, challenges arise in cyber response. The European framework and proofs-of-concept for the EU-GUARDIAN project aims to develop a reliable AI-based solution focusing on semi-automatic or automatic detection, mitigation, and response to security challenges, supporting analysts and decision-makers, enhancing cyber situational awareness and military infrastructure resilience.**

***Index Terms*—Cyber defence, Incident management, Artificial Intelligence**

Tipo de contribución: *Investigación en desarrollo*

I. Introduction

One of the most significant beneficiaries of Artificial Intelligence (AI) adoption is incident management. AI's ability to automate workflows results in smarter and more efficient operations, freeing IT team members to focus on other critical tasks [1]. AI contribute to developing more sophisticated security measures, allowing organizations to proactively identify and address potential threats and vulnerabilities. Additionally, AI-driven analytics can provide valuable insights into the constantly evolving threat landscape, enabling IT teams to adapt and refine their strategies to maintain a robust defence against emerging cyber threats [2]. However, integrating AI into real-world cyber response, particularly in the context of Cyber Defence actions, implies challenges [3].

To solve these challenges, the primary goal of the European framework and proofs-of-concept for the intelliGent aUtomAtion of cybeR Defence Incident mAnagemeNt project (EU-GUARDIAN) [4] is to develop a cutting-edge, precise, and dependable AI-based solution for automating significant portions of incident management and cyber defence processes. EU-GUARDIAN aims to investigate and establish the groundwork for promoting EU autonomy in developing and capacitating AI-based resources.

II. EU-GUARDIAN framework

The overall framework architecture is depicted in Fig. 1, showing the three main functional blocks: 1) **Capabilities for cyber defence incident management**, which involves four different streams. Monitoring functions to collect and analyse data from various sources. Detection capabilities are used to identify and analyse the nature and scope of any potential security breach or cyber-attack. Decision tasks are employed to analyse and evaluate security incidents to determine the appropriate response. To enhance the reaction to cyber incidents, EU-GUARDIAN explores various key points through the application of AI technology. 2) **Military mission support and situational awareness**. EU-GUARDIAN aims, by design, to enrich the cyber capabilities of the military apparatus. It is therefore considered to study how EU-GUARDIAN would be integrated into military planning; improve the cyber capabilities available to commanders; how it could be introduced into doctrine; facilitate autonomous incident management; enhance monitoring and analysis of operations; and how it would affect more traditional Command and Control (C2). Using EU-GUARDIAN would allow for a more integrated and dynamic image of the Cyber Common Operational Picture (CyCOP). A major effort will focus on the EU-GUARDIAN CONOP (Concept of Operation), specifying what it is and how it could be integrated into a military operation. Finally, it can be assured that an advanced AI tool can be a very promising enabler for assisting the cyber commands and motivating a better understanding, leading to better decisions. 3) **Metacognition and Layered Automation for cyber response**. A prompt and effective response to a cyber threat requires comprehensive situational awareness. Moreover, it is essential to ensure sustainability at both technological and

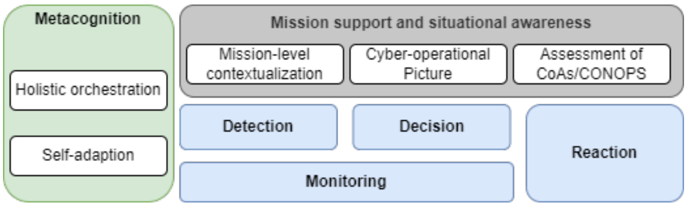
Metacognition
Holistic orchestration
Self-adaption
Mission support and situational awareness
Mission-level contextualization
Cyber-operational Picture
Assessment of CoAs/CONOPS
Detection
Decision
Reaction
Monitoring

Fig. 1. EU-GUARDIAN general architecture

human levels. For this aim, EU-GUARDIAN will adopt the strategy of breaking up the AIenabled power into smaller layers, which is referred to as metacognition layering. The project framework will have a holistic understanding of the operations and decision-making processes, using the self-regulatory cycle is inspired by the Self-Organizing Network (SON) paradigm, which aims to automate the management and optimization of Communication and Information Systems (CIS) assets.

III. Vision of a cyber defence project

The EU-GUARDIAN project is focused on innovating the capacities of the European defence industry by using AI and automatisms to transform intelligence into action at an IT and mission level. The project aims to build an accurate and reliable AI-based solution that manages and automates substantial parts of incident management and cyber defence proceedings. It is being developed within a European socio-political context to investigate the landscape, needs, and opportunities on the political, social, and cognitive fields transversal to adoption of disruptive capabilities and operation on cyber defence enabled by AI-based automation. The use of AI and autonomous systems in military decision making and war manoeuvre is becoming increasingly important, allowing for faster and more efficient operations. EU-GUARDIAN also explores the impact of PMESII and cognitive effects influence on the outcome of a cyber operation, making it possible to effectively assess the adversary's psychological disposition through AI-based technologies and counter the adversarial use of information.

An important topic to be handled during the project development is the rapid advancement of technology that has given rise to the concept of "dual-use technologies", which means that a single technology has applications in both civil and military domains. The dual-use nature of certain technologies presents unique challenges and concerns, necessitating a deeper understanding of the concept and its implications. These technologies have the potential to revolutionize industries, enhance national security, and contribute to economic growth. In the civilian sphere, cyber defence technologies are essential for safeguarding critical infrastructure, securing sensitive data, and ensuring the privacy. Businesses, governments, and individuals rely on a range of tools and techniques to protect their digital assets and maintain the integrity of their systems. Concurrently, the military domain is investing in advanced technologies and strategies to defend against cyber attacks, conduct offensive cyber operations, and maintain situational awareness in the rapidly evolving digital battlefield. For its part, AI technology is increasingly being integrated into military cyber defence capabilities as another important dual-use technology [5]. However, the dual-use aspect of cyber defence technologies raises concerns about the potential for proliferation, misuse, and unintended consequences, being crucial to establish appropriate regulatory frameworks, such as the European Dual-Use Regulation No 821/2021 [6], which strikes a balance between preventing the proliferation of WMDs, AI and related technology while ensuring the smooth functioning of the European single market.

IV. Other related projects

EU-GUARDIAN builds on lessons learned from previous European Defence Industrial Development Program (EDIDP) projects[1,2], where significant gaps related to the adoption of AI and Automation in the capabilities have been identified. Various EDIDP projects can be found in [7], as well as locating the objectives and scale, among others, of this program on cyber defence affairs. There a list of projects[3,4,5,6] with a tight linkage to several of the objectives proposed in EU-GUARDIAN that will be taken into account.

V. Conclusions and future work

In this paper, the main research and development goals of the EU-GUARDIAN project have been presented as an effort to address today's digitalization challenges in the defence sector. AI and Automation are opening new venues across different sectors including military applications. The EU-GUARDIAN project is committed on providing a reliable AI framework with the specific goal to automate large parts of cyber incident response management in military environments. Future work is focused on deepen into the definition of concepts and principles closely aligned with the military doctrine before delving into design phase and later feasibility analysis.

Acknowledgements

Funded by
the European Union

This project has received funding from the European Defence Fund (EDF) under grant agreement: Nº EDF-2021-CYBER-R-CDAI-2

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.responsible for any use that may be made of the information it contains.

References

[1] N. Kaloudi and J. Li, "The AI-based cyber threat landscape: A survey," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–34, 2020.

[2] H. Sedjelmaci *et al.*, "Cyber security based on artificial intelligence for cyber-physical systems," *IEEE Netw.*, vol. 34, no. 3, pp. 6–7, 2020.

[3] Z. Zhang *et al.*, "Artificial intelligence in cyber security: Research advances, challenges, and opportunities," *Artif. Intell. Rev.*, vol. 55, pp. 1029–1053, 2022.

[4] The EU-GUARDIAN project, "European framework and proofs-of-concept for the intelliGent aUtomAtion of cybeR Defence Incident mAnagemeNt." [Online]. Available: https://www.eu-guardian.eu

[5] H. Ueno, *Fusion of machine learning paradigms*. Springer, 2023, ch. Artificial intelligence as dual-use technology, pp. 7–32.

[6] Council of European Union, "Council regulation (EU) no 821/2021," 2021. [Online]. Available: http://data.europa.eu/eli/reg/2021/821/oj

[7] EU Defence Industry, "The EDIDP awarded projects." [Online]. Available: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-industrial-development-programme-edidp_en

[1] https://www.ecysap.eu

[2] https://www.cyber4de.eu

[3] https://ai4def.com

[4] https://ec.europa.eu/commission/presscorner/detail/en/fs_20_1081

[5] https://blogs.upm.es/rsti/2021/01/11/cobra-realistic-traffic-and-network-simulation-environment-for-cyber-defence-training/

[6] https://www.pandora-edidp.eu