EUROPEAN
DEFENCE
AGENCY

EDA RESEARCH, TECHNOLOGY, AND INNOVATION PAPERS AWARD

2023

EUROPEAN
DEFENCE
AGENCY

CONTENTS

FOREWORD

Dear Reader,

The challenges facing our security and defence are increasingly complex and multifaceted, and require new approaches and solutions. As we enter an era of geopolitical uncertainty and emerging threats, we must remain committed to investing in the research and development of new defence technologies. Only by doing so can we ensure that we are prepared to meet the challenges of tomorrow and protect the safety and security of our citizens.

At the European Defence Agency, we are committed to fostering a culture of innovation and collaboration, and to promoting the exchange of ideas and best practices among stakeholders. Innovation is at the core of the European Defence Agency's mission to strengthen the defence capabilities of Member States. To this end, the Agency has been organizing the EDA Defence Innovation Prize since 2018, rewarding disruptive technologies, products, methodologies, or services applicable in the defence domain. These prizes have been dedicated to specific topics, incentivizing non-traditional EU defence stakeholders to introduce and implement their innovative solutions in the defence sector. The most promising proposals have been brought forward in the Agency's extensive network, contributing towards greater defence innovation in Europe.

Against this backdrop, the contributions of the academic community are also critical to achieving our common goals. It is thus my pleasure to introduce this collection of innovative ideas from the academic community, which represents a rich source of knowledge and expertise for the European defence sector. This year we have launched our very first EDA Research, Technology, and Innovation Papers Award, aiming to promote and support the work of early career researchers by introducing their work to the defence community.

This Booklet showcases the results of the 2023 EDA Research, Technology, and Innovation Papers Award contest, which focused on innovative technologies, processes and applications for enhanced future defence capabilities. The contest attracted a diverse range of innovative ideas from early career researchers, academia and other entities.

The proposals presented in this Booklet provide insights into potential directions for the future of defence in the EU. They highlight the importance of domains such as situational awareness and communication and information systems in enhancing defence capabilities and offer cutting-edge solutions to address these challenges. By fostering collaboration and innovation across the EU defence community, we can accelerate the development and implementation of these ideas, ensuring that our armed forces remain at the forefront of technological advancement.

Looking ahead, it is clear that innovation will continue to be a critical factor in the defence sector. The EDA will continue to promote and reward innovation through activities such as this novel EDA Research, Technology, and Innovation Papers Award contest, and other activities planned in the framework of the new Hub for EU Defence Innovation (HEDI).

Working and inspiring new breakthroughs for a peaceful future,

Jean-François RIPOCHE
EDA Research, Technology and Innovation Director

EDA DEFENCE INNOVATION: AN EYE ON THE EDA RESEARCH, TECHNOLOGY, AND INNOVATION PAPERS AWARD 2023

Panagiotis Kikiras[1] and Fabrizio Berizzi[1]

ABSTRACT

Innovation has become central for governments, industry, and academia as an instrument to facilitate growth. This includes the creation of a new concept/technology/ product/process or service, as well as the application of existing technology to a different problem or domain. Anyway, innovation is not only focused on the creation of new concepts. Although related to the research innovative ideas, it is also focused on the value that the new concept will create for end-users. In this regard, innovation in the defence sector should aim at enhancing military capability. To foster innovation in the defence sector, EDA has introduced a set of tools and initiatives in order to act as a catalyst in the innovation process. One of these tools is the Research, Technology, and Innovation (RTI) Papers Award 2023. The editorial at hand provides an overview of the innovation award and provides some additional insights on the innovation framework of OSRA and innovation activities in EDA in general.

KEYWORDS

EDA, Innovation, Research, Defence, HEDI, OSRA, CAPTECH

1. INTRODUCTION

Research & technology (R&T) is at the heart of defence capability development and, therefore, one of the EDA's top priorities [1]. The effectiveness of tomorrow's defence depends on today's investment in new capabilities. To that end, Member States must remain at the cutting edge of defence innovation and research.

Given the magnitude of the task and the shortage of research funding at national levels, Member States are rightly seeking synergies and cost benefits from collaborative projects at European level, notably through EDA.

To ensure the identification of technology gaps and common areas of interest for cooperation, the Overarching Strategic Research Agenda (OSRA) [2], the EDA R&T planning tool, developed together with its Member States, provides a shared vision of the most important technical challenges to be researched at European level within the CapTech areas.

With its specialized Capability Technology Groups ('CapTechs') composed of national governmental experts, industry and research organisations, EDA offers Member States a tailor-made platform where they can voluntarily engage in collaborative defence research projects which are of interest to them. Since its creation in 2004, EDA has managed some 250 R&T projects, worth over €1 billion [3].

EDA also ensures that Member States make best use of existing and upcoming EU funding for defence-related research, especially the European Commission's Preparatory Action on Defence Research (PADR) which is managed by EDA and provides inputs to a fully-fledged EU Defence Research Programme under the European Defence Fund (EDF) [4] as of 2021.

[1] European Defence Agency, Brussels, Belgium

2. EDA OSRA INNOVATION FRAMEWORK AND HEDI

2.1. OSRA INNOVATION FRAMEWORK

Innovation can be perceived as the creation and application of new products, services, and processes. Nevertheless, innovation is not only focused on the creation of new concepts. It also focuses on the value that the new concept will create for end-users. In this regard, innovation in the defence sector should aim at enhancing military capability [5].

Innovation can be considered in different ways;

1) Disruptive innovation is one which radically changes the way of operation ("of doing things"), and therefore has a significant impact also for the defence sector, on the way in which armed forces operate.

2) Incremental innovation concerns an existing product, service, process, organisation, or method to significantly enhance or upgrade its performance.

Evidently, successful defence innovation requires both disruptive innovation and capability-based incremental innovation in order to provide MS with needed defence capabilities for the future.

While it might seem to be an oxymoron to discuss innovation process, best practices are indicating that a structured process to drive innovation is a prerequisite and without it there is only little chance of collecting great innovative ideas to be further developed. Nevertheless, although a predictable, repeatable innovation process is needed, the process should be fairly light not to inhibit innovation.

EDA has conducted a wide analysis of innovation strategies and systems of 32 States including non-EU, of organisations with similar to EDA's scope such as ESA and DARPA and of innovative non-defence companies such as Amazon and Alphabet especially in terms of the methodological tools they are using to foster innovation from rigid to more flexible starting by the Kline model [6], followed by Double Diamond [7] and Design Thinking [8], and ending with Blue Ocean [9].

In this direction since 2016 EDA has developed a lightweight innovation framework which has been built on the following principles:

- Cultivate innovation culture.
- Establish idea acquisition and management processes.
- Engagement with research, innovation, and industrial stakeholders
- Explore and promote activities in the 3 principal elements characteristic to any innovation system (capital / talent / knowledge)

Based on those principles the OSRA innovation framework has been developed consisting of three work strands:

- identification of innovative ideas and innovators
- outreach to increase awareness of the solutions produced and their application to the defence and dual - use domains.
- implementation of these ideas using all available funding instruments.

While building the aforementioned innovation framework, EDA has launched, a number of internal and external activities. Internal activities are aiming mainly in transforming the existing processes and activities to be more "innovation friendly", while external activities are focusing mainly on extending the reach and nursing of the defence innovation ecosystem.

The core of the internal activities aimed at the CapTechs. As they are the technical communities where strategic research agendas match the key input to OSRA, and the Technology Building Blocks roadmaps are built. This includes a number of activities especially in the area of ideation, systematic innovative technology identification and foresight, and extension of CapTech communities by organising innovation challenges aiming at attracting no traditional defence players. Until today EDA organised five challenges with the 6th recently announced. This year, the EDA Defence Innovation Prize 2023[10] focuses on innovative, defence-related ideas in the categories of Technologies for Situational Awareness and Technologies for Communication and Information Systems.

As far it concerns the lessons learned from the implementation of the OSRA Innovation Framework the most important and relevant for developing defence innovation ecosystems are the following:

a. Need for an agreed vocabulary - because innovation means different things to different people/communities.

b. Need for an agreed scope – the successful innovation needs a purpose. Especially in defence innovation is targeting the creation of Military Value meaning delivering Military Capabilities. This capability driven approach can be divided in 3 planning horizons.

    i. In short term where a mature innovative solution exists and requires small adaptations for inserting it into existing platforms or systems,

    ii. in mid-term where we are dealing with emerging threats and the scope of innovation is to mature existing solutions from other fields and therefore reducing the risk of investing on "new technologies and

    iii. in long term where the requirements of future operational scenarios versus the existing solutions revealing a strategic gap which needs to be covered by future technologies.

c. Need to build the ecosystem and change the mindset of all stakeholders - innovation does not happens in vacuum! It requires changing the mindset of involved stakeholders and cultivation of appropriate environment and support by the top management.

d. Need for a clear governance- Innovation is a process and as such it can be manage by using appropriate tools and methodologies.

In order to better capitalize on the experience gained and the lessons learned and to correspond to the rapidly changing political and security and defence environment in Europe and the world [11], the EDA innovation activities evolved under the umbrella of European Hub for EU Defence Innovation (HEDI) [12].

2.2. HEDI – THE EVOLUTION OF EDA INNOVATION FRAMEWORK

HEDI operates at the intersection of EDA's already existing innovation activities, serving as a catalyst and amplifier. HEDI's activities will contribute to and focus on the agreed EU priorities for capability development (Capability Development Plan [13]), defence research (Overarching Strategic Research Agenda) as well as skills, technologies, manufacturing capabilities (Key Strategic Activities [14]). Three steps have been defined for the Hub to grow to fulfil its role and potential as catalyst and amplifier of defence innovation at EU level:

- The first step will inspire and promote innovation at the European level: the Hub will focus on networking and situational awareness activities. It should be considered as a ramp-up phase, making the most of existing EDA resources.
- The second step will allow the Hub to be operational across all activities and services identified in the initial portfolio. This will set the Hub at the heart of facilitating defence innovation across Member States and EU institutions.
- The third step, HEDI 2.0 is proposed as a way to to reach the full potential of the Hub as an EU-wide platform for cooperative design and experimentation embedded in the EU capability development process and has to be further defined and decided at a later stage.

2.2.1. HEDI ACTIVITIES AND SERVICES

To facilitate its role the initial portfolio of the HEDI services has been organised in six clusters of activities:

- **Common Picture:** HEDI will contribute to creating a common picture on defence innovation, including but not limited to best practices, methodologies, experiences, les- sons identified and learned, specific projects, initiatives, and status of play on Emerging and Disruptive Technologies. It will set up and manage networks of defence innovation organisations and researchers, who will be invited to exchange views on these topics once or twice a year. These exchanges will further support the professionalisation of defence innovation and scale up defence innovation activities across Europe. The activities within this cluster will be organised in cooperation with the European Commission.
- **EDA Innovation Prizes:** Innovation prizes are a way to collect a pool of innovative ideas and solutions at all Technology Readiness Levels to fill identified gaps and needs. The winners of the prize are provided with seed funding to work on a plan for the development of their ideas towards proof-of-concept or demonstrators. Although the innovation prize is an already established modus operandi at EDA, the establishment of the HEDI will reinforce this activity not only by increasing the number of prizes awarded and the number of domains covered, but also by accelerating the uptake of innovation into capabilities. Innovation prizes address the initial phase of innovation in which it is key to exploring many different technical solutions with the full spectrum of actors, from start-ups and SMEs to prime contractors.
- **Innovation challenges:** Challenges and Hackathons are a specific R&T methodology targeting short cycles of development from proof-of-principle to minimum viable product. These methodologies have proved effective in attracting non-traditional defence players due to their short and focused nature and their lower initial threshold of access. HEDI in cooperation with partners, will select innovations suitable for this approach based on outcomes of other activities (e.g., innovation prizes) or specific capability gaps identified by Member States.
- **Proof-of-concept/demonstrators:** Making use of EDA flexible contractual framework and selecting the most suitable funding stream, HEDI will advance the development of the technologies showing the most potential in terms of performance and receiving the most support from potential users.
- **European Defence Innovation Shows:** An important dimension in the innovation funnel is the need to have a platform to increase awareness about the European defence innovation ecosystem, disseminate project results and connect stakeholders. HEDI will organise yearly a series of shows combining exhibitions and projects outcomes, conferences, panel discussions and prize awards.
- **Uptake of innovation:** To ensure a coordinated and harmonised uptake of innovations into capabilities, taking into account all dimensions DOTMLPFI (Doctrine, Organisation, Training, Materiel, Leadership and Education, Personnel, Facilities and Interoperability) and paving the way towards an initial operational capability, HEDI will explore the potential to organise multination Concept, Development, Experimentation and Concurrent Design campaigns based on participating Member States' priorities.

Within this HEDI framework, EDA launched the 2023 EDA Research, Technology, and Innovation Papers Award 2023.

3. THE EDA RESEARCH, TECHNOLOGY, AND INNOVATION PAPERS AWARD 2023

The European Defence Agency (EDA) issued on 1 February 2023 its call for applications to its first ever EDA Research, Technology, and Innovation Papers Awards. This contest will reward a total of three original and valuable defence-related papers covering technologies, processes and applications for enhanced future defence.

Through the "EDA Research, Technology and Innovation Papers Award 2023" contest, the European Defence Agency (EDA) aims at:

- Promoting and support the work of early career researchers by introducing their work to the defence community,
- Stimulating engagement of innovators to accelerate access to emerging and potentially disruptive research,
- Identifying areas in which additional investment is needed to fully address future defence capability needs and
- Identifying different ways to cover current defence needs and gaps.

In total twenty papers have been submitted from early career researchers covering different defence technologies and application domains ranging from sensors to Artificial Intelligence (AI) systems. The domains covered are depicted in Figure 1 showing the word cloud of the keywords as entered by the authors of the submitted papers.

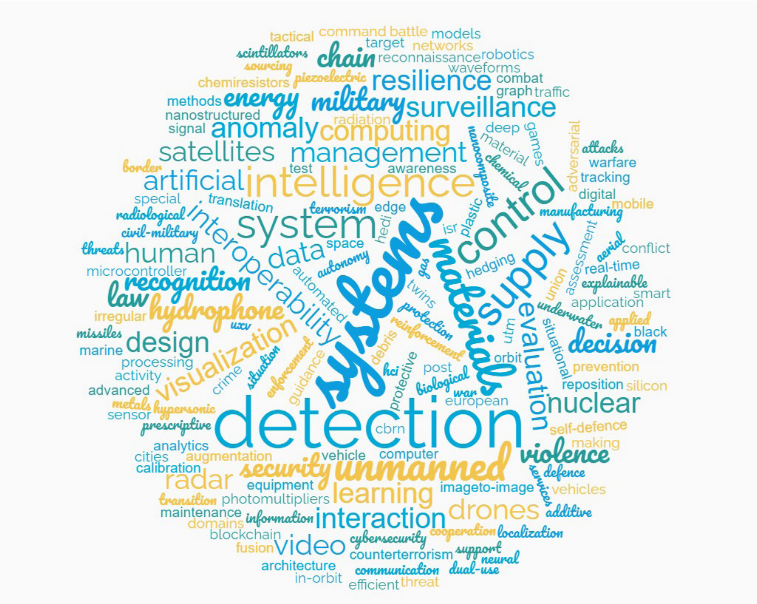


Figure 1. Word cloud of the submitted Keywords.

Concerning the demographics of the submissions in total the main authors came from 9 Member States (see Figure 2 and Figure 3) and from institutions across EU (see Figure 4) from which it is evident that most of them (approximatively 65%) are still on academic institutions and RTOs.

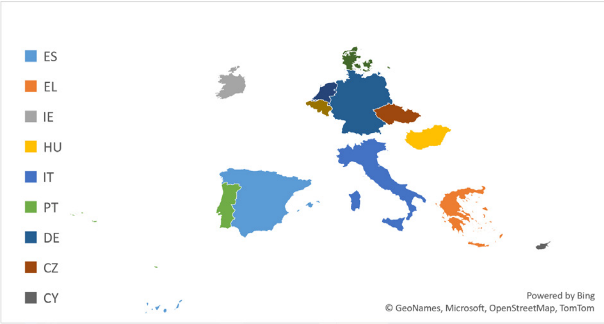


Figure 2. Nationalities of main authors

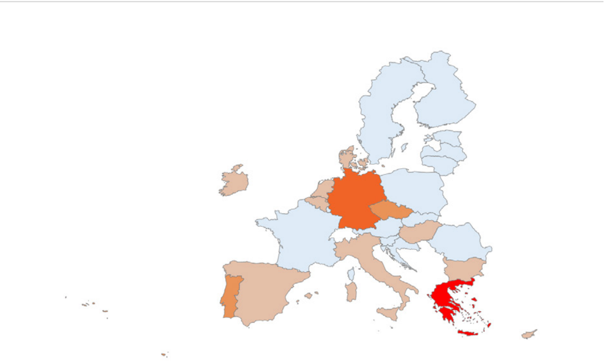


Figure 3. Total number of authors per MS

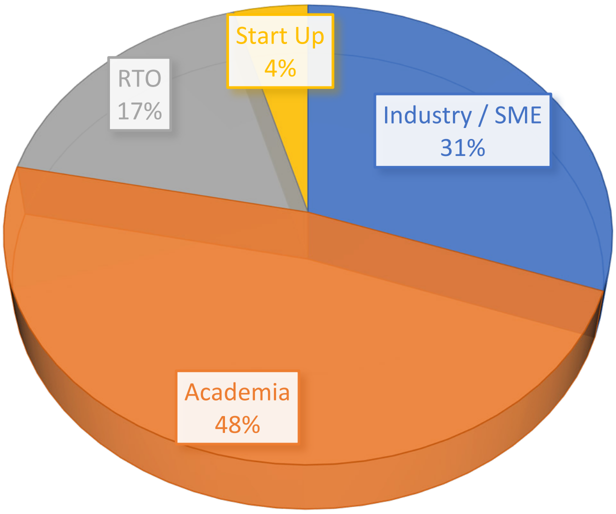


Figure 4. Distribution of Authors on types of Institutions.

As far it concerns the papers of this volume a brief overview is listed below. Please note that out of the 20 papers only 18 are included based on the rules regarding the participation to this contest.

Title	Overview	Authors
Battle Operational–Strategic Decision-Making; a Disruptive Framework	This paper proposes a disruptive framework that overcomes most limitations of traditional models and supports decision-making at the highest command levels: the strategic and the operational ones, resorting to the determination of the decay of combat force levels, commonly referred to as attrition (losses), as a mechanism for evaluating decisions.	Gerardo Minguela Castro
Towards a New Symbology and Visual Interaction Design for Sub-Sea Military Operations	This paper proposes extending existing NATO military standards with the creation of a comprehensive proposal for a new Sub-sea symbology and visual interaction design framework for sub-sea military operations (SSMOs).	G. Walsh, N. S. Andersen, N. Stoianov and S. Janicke
League of algorithms: a novel data augmentation approach to build a training dataset for image-to-image translation problems	This paper presents a mobile radiation detection system based on plastic scintillators with silicon photomultiplier sensors for the detection and localization of gamma, beta, and neutron sources/materials	Niccolò Camarlinghi, Antonio Di Tommaso, Benedetto Michelozzi, Giacomo Fontanelli, Andrea Masini
A Tiered Service For Interoperable Data Ingestion and Distribution	This paper is based on an innovative tiered architecture, which guarantees secure ingestion and distribution of data (extracted from heterogeneous sources) during a post-conflict phase. The use of AI-based trust and risk models - together with solutions for protecting data domains transitions - is demonstrated to allow for reliable data quality check and data protection.	Björn Appel, Fulvio Arreghini, Frank Beer, Dennis Füller, Peter Gorski

GNN-based Deep Reinforcement Learning with Adversarial Training for Robust Optimization of Modern Tactical Communication Systems	This paper investigates the feasibility of a Graph Neural Network (GNN)-based Deep Reinforcement Learning (DRL) for tackling complex optimization problems in modern communication systems deployed to tactical networks.	Johannes F. Loevenich, and Roberto Rigolin F. Lopes
Additive Manufacturing Application For Resilience in Defence Supply Chains: Pooled Capacity Hedging as a Hybrid Instrument	This paper addresses the question how defence supply chains can become more resilient. Additive Manufacturing (AM) is presented as an enabling technology to increase resilience. Although there is always room for technical improvement, this research focuses on an intelligent application of AM in digital supply chains.	Andreas Glas and Michael Essig
Green Energy Resilience Against Missile & Drone Attacks – Economics of Targeting Wind & Solar Energy	This paper focuses on the Resilience of Solar and Wind energy infrastructure, from an "economics of war" perspective, when faced with the threat of missile and drone attacks. The pertinence of this paper derives not only from the objectives of the European Clean Energy Transition, but additionally from updated energy security concerns related to the targeting of critical energy infrastructure in Ukraine.	Pedro Gonçalo Rodrigues
Swarming: A Disruptive, Game Changing Technology for Defense Applications	This paper describes European activities in swarming and provides insight on the game-changing impact it can have for the defence and civilian sectors.	Vaios Lappas, Ioannis Daramouskas, Nicki Patrinopoulou, Dimitris Meimetis, Vassilis Kostopoulos
Prescriptive Auto-Maintenance Architecture for Trustworthy Cross-Domain-Implementation in Tech-Defense	This paper presents an innovative Prescriptive Auto-Maintenance Architecture (PAMA) for dependable cross-domain implementation in defense technology, designed to optimize performance, reduce maintenance costs, and increase overall equipment reliability in response to the abovementioned challenges.	Vasiliki Demertzi and Stavros Demertzis
Revolutionising CBRN Defence through Nanotechnology-based Encapsulation of Conducting Copolymers within PAMAM Dendrimers	This paper presents the development of advanced nanocomposite materials for Chemical, Biological, Radiological, and Nuclear (CBRN) defence applications by encapsulating conducting copolymers of polyaniline, polythiophene, and polyacetylene within polyamidoamine (PAMAM) dendrimers.	Elçin Tören
How drones can enchance counter terrorism capabilities	This paper reviews the legal, ethical, and safety concerns associated with the use of counterterrorism drones in the EU, suggests a viable solution, and highlights the need for policymakers to carefully consider the long-term effects of their counterterrorism strategy and to ensure that drones' use is consistent with international law and human rights standards.	Christos Chatzis, Xesfingi Eleni and Karampelas Vasileios

A Modular App Store Reference Architecture (MASRA)	This paper is to present a reference architecture for the creation of an Interoperable AppStore (the "MASRA") which enables the delivery of additional value (operational benefits) by the combination of functionalities among its hosted applications	Demetris Antoniou, Stylianos Koumoutzelis, Titos Georgoulakis , Emmanouil Kafetzakis, Ioannis Giannoulakis
The Strategic Promise of Digital Twins to Enhance Supply Chain Resilience	This paper argues that it is feasible to make (military) supply chains less redundant through the adoption of digital twins as a technological solution.	Monica Adami, Mateusz Nowak, Maarten Toelen, Claudio Valle, Arno Van der hasselt, Annika Weinmann
Design and Development of the Next Generation, Low-Cost and High-Sensitivity Hydrophone for Critical Underwater Intelligence Applications	This paper, the development of a low-cost hydrophone operating at a frequency range of 0.1 Hz to 100 kHz, is presented. Moreover, an electronic circuit was designed and prototyped, to improve hydrophone's performance and digitize its output, in order to perform further signal analysis through a personal computer.	Nefeli Motsi, Georgia Stamou , Spyridon Angelopoulos and Evangelos Hristoforou
Gas Sensors Equipped with Black Metal Active Layers	This paper is focused on study, fabrication and application of highly sensitive gas sensors working as chemiresistors, equipped with black metal active layers. The term "black metal" denotes a specific form of metallic material with extremely high porosity, gas sorption capacity and catalytic activity.	Jan Kejzlar
Improved Detection of Hypersonic Threats with Radar Using Irregular Waveforms and Advanced Processing	This paper demonstrates the potential of irregular waveforms and advanced processing for the detection of hypersonic threats. It is shown that their combination can significantly increase the detection performance and the measurement accuracy compared to multiple, medium pulse repetition frequency waveforms with linear signal processing.	Pepijn Cox, Keith Klein, Mario Coutiño, and Laura Anitori
Defence oriented Test & Evaluation Capabilities as accelerator for innovation in a triple helix environment for Marine Robotics and Underwater application	This paper presents ongoing and developing projects that aim to enhance the capabilities of maritime systems through the use of autonomous vehicles.	LT Francesco Cannarsa, LT Davide Cosimo, LT Lorenzo Bazzarello, LT Daniele S. Terracciano, Capt Navy (retd) Mirko Stifani
A Mobile Radiation Detection System for Security and Defence	This paper presents a mobile radiation detection system based on plastic scintillators with silicon photomultiplier sensors for the detection and localization of gamma, beta, and neutron sources/materials	Luís Miguel Cabeça Marques, Alberto Manuel Martinho Vale, and José Pedro Miragaia Trancoso Vaz

Table 1. Description of the contents of the volume.

4. CONCLUSIONS

Innovation is a continuous process and to be successful it requires a few supporting actions. One of key initiative going to this direction is the abovementioned proposed innovation framework as enhanced by the creation of HEDI and the services that it will be managing.

EDA, with the support of the Member States, will continue developing services that will be aiming at strengthening the European Defence Innovation ecosystem at all levels of its value chain ranging from giving the opportunity to young innovators to present their ideas with activities like this EDA Research, Technology, and Innovation Papers Award, to Research Technology Organizations (RTOs) and Industries to present their innovative defence applications to innovations prizes and challenges.

REFERENCES

[1] EDA website: https://eda.europa.eu/what-we-do/eda-in-short - Last accessed 12.03.2023.

[2] EDA website: OSRA factsheet - https://eda.europa.eu/docs/default-source/eda-factsheets/2019-03-25-factsheet-osra6175b73fa4d264cfa776ff000087ef0f.pdf - Last accessed 12.03.2023

[3] EDA website: Capability Technology Group (CAPTECH) https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-(captechs) - Last accessed 12.03.2023

[4] European Defence Fund (available online) https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf_en - Last accessed 12.03.2023

[5] Disruptive Defence Innovations (available online) https://eda.europa.eu/webzine/issue14/cover-story/disruptive-defence-innovations-ahead - Last accessed 12.03.2023

[6] Wiles, Rose, Graham Crow, and Helen Pain. "Innovation in qualitative research methods: A narrative review." Qualitative research 11.5 (2011): 587-604.

[7] Gustafsson, Daniel. "Analysing the Double diamond design process through research & implementation." (2019).

[8] Baker III, Fredrick W., and Sarah Moukhliss. "Concretising design thinking: A content analysis of systematic and extended literature reviews on design thinking and human-centred design." Review of Education 8.1 (2020): 305-333.

[9] Leavy, Brian. "Value innovation and how to successfully incubate "blue ocean" initiatives." Strategy & Leadership(2018).

[10] EDA 2023 Innovation Prize (available online) https://eda.europa.eu/what-we-do/research-technology/innovation-prize - Last accessed 12.03.2023

[11] EU Strategic Compass (available online) https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en - Last accessed 12.03.2023

[12] European Hub for Defence Innovation (available online) https://eda.europa.eu/docs/default-source/brochures/hedi-factsheet-(final).pdf – Last accessed 12.03.2023

[13] EDA Capability Development Plan – (available online) https://eda.europa.eu/docs/default-source/brochures/cdp-brochure---exploring-europe-s-capability-requirements-for-2035-and-beyond.pdf - Last accessed 12.03.2023.

[14] EDA Key Strategic Activities – (available online) https://eda.europa.eu/what-we-do/EU-defence-initiatives/priority-setting/key-strategic-activities - Last accessed 12.05.2023

BATTLE OPERATIONAL–STRATEGIC DECISION-MAKING; A DISRUPTIVE FRAMEWORK

G. Minguela Castro, PhD[1]

Abstract

Armies have always felt the need to base their decisions on proven operational research methods that seek to provide the command with alternatives in the decision-making process, from optimization of operations to strategic evaluation and cost economics. Battle casualties are a subject of study in military operations research, which applies mathematical models to quantify the probability of victory vs. loss. In particular, different approaches have been proposed to model the course of battles. However, none of them provide adequate decision-making support for high-level command. To overcome this situation, this paper proposes a disruptive framework that overcomes most limitations of traditional models and supports decision-making at the highest command levels: the strategic and the operational ones, resorting to the determination of the decay of combat force levels, commonly referred to as attrition (losses), as a mechanism for evaluating decisions. The framework applies adaptive and predictive control engineering methods to dynamically adjust to changes in the battle, taking into account the capabilities and maneuvers of the adversary and the effects produced. Also, it includes a learning mechanism to improve decisions under conditions with high uncertainty.

Keywords

Decision support systems, Combat models, Battle situation, Warfare information system, and War games.

1. INTRODUCTION

Lanchester's seminal work [1] on battle dynamics' modeling has inspired significant research on the development of combat abstractions to support military decision-making under uncertainty, pursuing how to achieve superiority in combat. Lanchester's original model and its distinct evolving extensions have dominated the dynamic assessment of conventional land force balance for a long time [2], being used by major organizations (e.g., the US Army, the Office of the Secretary of Defense, etc.) to assess a wide variety of issues (e.g., evaluating the balance of operation theater [3, 4], guiding decision on weaponry choices [5], etc.).

Nevertheless, it is worth noting that Lanchesterian models have important limitations, e.g., they perform an oversimplistic one-side treatment without taking into account the opponent's capabilities, and they cannot be used for disaggregated engagements [6].

Another matter to be taken into account is the abstraction level supported by the decision-making procedures. Military doctrine usually distinguishes the following three levels of command:

1. The strategic level studies the conflict from the most abstract perspective, considering the war final outcomes as a whole. It involves the overall planning, resource distribution, and organization of the military force. Additionally, it defines and supports the national policy.
2. War is divided into campaigns, which are organized into operations. The operational level deals with the design, arrangement, and execution of campaigns and principal operations.
3. The Tactical level implements the campaign operations on the battlefield.

Interestingly, most decision-making approaches, including the non-Lanchesterian ones, are focused on the tactical

[1] 1Digital Trasnformatión Deparment, Isdefe, C/Beatriz de Bobadilla,3, Madrid, Spain, gminguela@isdefe.es

level of command [6,7]. In other words, the operational and strategic levels of command are insufficiently supported by existing decision-making systems.

This paper proposes an innovative framework that overcomes most limitations of Lanchesterian models and supports decision-making at the highest command levels: the strategic and the operational ones. Our framework applies adaptive and predictive control engineering methods to dynamically adjust to changes in the battle, taking into account the capabilities and maneuvers of the adversary and the effects produced. Additionally, it includes a learning mechanism to improve decisions under conditions with high uncertainty.

Finally, the paper reports the empirical evaluation of our framework on the Battle of Creta, Iwo Jima, and Kursk. This, by itself, constitutes a relevant contribution as most literature on military decision-making lacks adequate experimental validations. In particular, most validations follow mathematical procedures that make non-realistic assumptions [8] or rely on simplistic made-up examples [9].

The remainder of this paper is organized as followings. Section 2 describes our frame- work and Section 3 reports its empirical validation. Finally, Section 4 provides some concluding remarks and discusses future challenges.

2. A FRAMEWORK TO SUPPORT BATTLE OPERATION STRATEGIC DECISION-MAKING

There are two principal battle analysis mechanisms alternative to classical Lanchester's models: (i) stochastic models and (ii) deterministic models, some of them in the Lachesterian tradition [10,11]. Currently, other approaches such as intelligent agents are gaining substantial momentum [12,13]. These new models aim to extend the capabilities [6,9] and reduce the shortcomings of previous approaches [14,15]. However, they fail to be an appropriate benchmark for high-level decision-making.

The framework overcomes the limitations of Lanchester's original work, which are profoundly discussed in [16, 6], by treating the battle as a cause-effect process that evolves according to the dynamics of the Lanchester's equations subject to changes and external actions. To do so, our approach applies the adaptive and predictive control theory introduced in [17], which incorporates uncertainty modeling techniques. Our approach architecture comprises a set of blocks that work cooperatively and ensure that decision-making is

carried out coherently, following the military doctrine. In particular, a set of sequential stages trigger the definition of the applicable strategy, the evaluation and selection of the different possible courses of action (COAs), and the adaptation of the model to the evolution of the operation.

Each block represents the mechanics of military thinking, see Figure 1, where **x(t)** and **y(t)** define the number of combatants of the x-force and y-force at each instant, **x(t + 1)e** and **y(t + 1)e** are the estimated the number of combatants for the following instant.

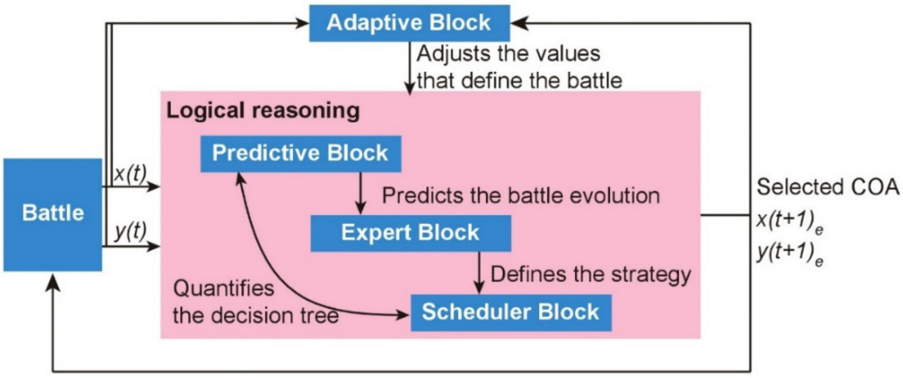


Figure 1. Architectural design of our framework. Each block represents the mechanics of military thinking, thus (i) assessing the events of the battle that will define the strategy to be followed and selecting the COA to accomplish the mission, (ii) identifying the resources that will be necessary to carry it out, and finally (iii) adapting to the outcomes.

The implementation requires a logical process capability and should simulate the decision-making process, from prediction to action. In this context, the new framework is formulated and tested (it will be robust if its application on real confrontations meets the expectation in terms of performance and consistency).

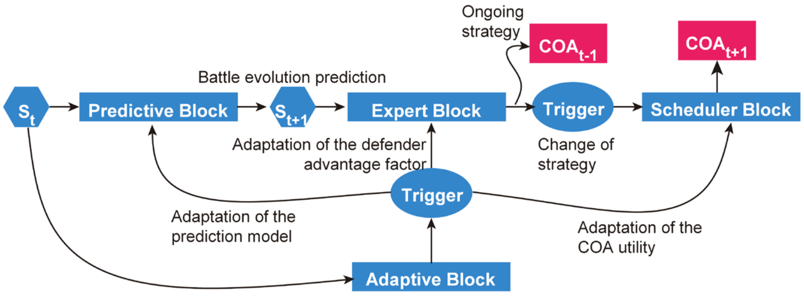

Ongoing strategy
COA t-1
COA t+1
Battle evolution prediction
S t
Predictive Block
S t+1
Expert Block
Trigger
Scheduler Block
Adaptation of the defender advantage factor
Change of strategy
Trigger
Adaptation of the prediction model
Adaptation of the COA utility
Adaptive Block

Figure 2 Primary elements that trigger the choice of a specific COA in the new framework through a sequential model.

Figure 2 develops the essential elements that iteratively trigger the choice of a specific COA. The predictive block generates the predicting evolution. The adaptive block adjusts the parameters of the constituent blocks based on the difference of the output signal (the actual situation) from the predicted one, suitably updated with the last executed COA. The expert block acts trying to modify the trend defined by the predictive block through the scheduler block, thus changing the course of actions following the needs of the battle. It is worth noting that the set-point is related to fulfilling the mission, that the action development times are operation times and, that the available databases with information on conflicts are usually represented by time evolutions in days, in the best case.

2.1. PREDICTIVE BLOCK

In military doctrine, intelligence is defined as the interpretation and integration of knowledge about the terrain, meteorology, population, activities, capabilities, and intentions of a present or potential enemy. The intelligence cycle is composed of the phases of direction, acquisition, elaboration, and dissemination. The predictive model will recreate this cycle in the prediction of scenarios necessary to evaluate future decision-making, where tactics, combat strength, and attrition are identified as the most critical factors for modeling the dynamic prediction of a confrontation. The predictive block defines the future trend of the confrontation at an instant after the current one using Lanchester's equations and a regression model.

2.1.1. STUDY AND CONCLUSIONS FOR THE PRACTICAL IMPLEMENTATION OF THE LANCHESTER COMBAT MODELS

The Lanchester's equations simplify battle attrition models, emphasizing the importance of troop concentrations in the final outcome. These models were developed during the Great War by F.W. Lanchester [18]. Since then there have been later developments of these laws such as [19] for the mixed law or [20] for the logarithmic law or [21] in his general law. Literature on Lanchester combat models has grown to provide new insight, thus; [22] analyzed the quadratic law using data from the battle of Inchon-Seoul (1950), concluding that the best fit occurred by dividing the battle into sub-battles; [23] studied the stochastic Lanchester form, concluding that other factors play an important role in real combat (strategy, environment, etc.) that the Lanchester's equations do not take into account; [24] contrasted daily casualties through data from the battle of Kursk (1943) using Bracken's general Law, concluding the need to divide battles into sequential phases differentiated by major changes in battle concentrations or strategy. Lanchester's models should be understood as a resource for decision-making of battle dynamics on a local (operational) scale. An explicit approach that seeks to understand, track and anticipate the direct and indirect effects of operational decisions. As the combat models are developed at different levels of abstraction, they can be represented together by Figure 3 where the Lanchester models should be positioned as a mechanism for evaluating decisions.

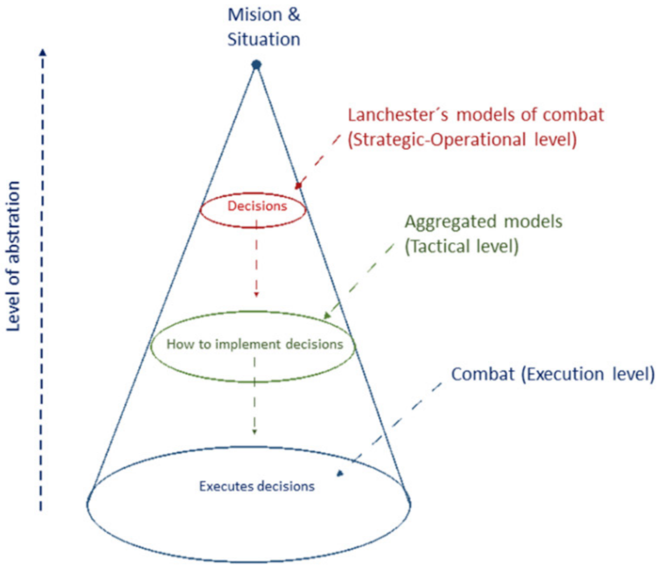


Figure 3. The vertical axis identifies the level of abstraction embodied in the model and the base circle of the cone represents reality or complete lack of abstraction, as the level of aggregation increases, the variables defining the level of command gradually abstract details of combat execution. Thus, in the level of application of Lanchester models is in line with levels of strategic-operational aggregation, aggregated models cover up the most basic execution mechanisms of the battle such as individual clashes and the execution level is affected by factors such as weaponry, position, visibility, logistics, etc.

Equations presentation

These equations consider two hostile forces, denoted as x and y. For simplicity, forces are typically modeled as the number of combatants, i.e., the size of each army, although it can be a representation of any element fully engaged in combat with the capacity to generate casualties or losses. Thus, x(t) and y(t) define the number of combatants of the x and y forces at instant t, t is usually measured in days from the beginning of the battle. Additionally, Lanchester's equations consider each force's lethality, denoted as a and b, whose calculation depends on the fire, combat typologies, and balance of forces.

Applying the generalized model defined by Bracken [21] into our approach (Equations (1) and (2)), it is possible to determine the nature of the battle empirically. We define p as the exponential factor of the attack force and q as the exponential factor of the defense force. Where **f(t)** and **g(t)** are the replacement forces or evacuated forces according to the sign.

$$\frac{dx}{dt} = -ay(t)^{p}\, x(t)^{q} + f(t) \quad (1) \qquad \frac{dy}{dt} = -bx(t)^{p}\, y(t)^{q} + g(t) \quad (2)$$

Defining p and q in the interval [0, 1],

- If ***p*** and ***q*** is (1, 1) it defines the linear law.
- If ***p*** and ***q*** is (1, 0) it defines the quadratic law.
- If ***p*** and ***q*** is (0, 1) it defines the logarithmic law.

It is work remarking that the tactical parameter d (offensive or defensive strategy) of Bracken's model [21] is not taken into account because it does not contribute substantially to the adjustment of parameters.

Lanchester models can be efficiently implemented thanks to the current availability of efficient numerical Ordinary Differential Equations (ODE) solvers. Also, they are easily interpretable, thus providing good support to decision-making on high aggregation command levels.

2.1.2. GENERALIZED REGRESSION MODEL

Regression attempts to explain the causality of the effects. The generalized model [21] generates four variables to be solved. Using (i) the least-squares method as target function and optimized by the Generalized Reduced Gradient (GRG) algorithm, hose mathematical structure of which can be analyzed in [25] and [26], searches for a feasible solution from an initial point and moves in search of the improvement of the Objective function (Equations (3)), from data obtained during the course of the battle, and (ii) the following metrics that account for the regression model quality: Sum of Squares Regression (SSR), Sum of Squares Total (SST) and R^2, it obtains a feasible estimation procedure to solve the four unknown variables. Therefore, the GRC algorithm manages the slope of the target function as the input values change and determines that it has reached an optimal solution when the partial derivatives are equal to zero. A higher R2 value indicates a better fit for the mean daily losses (estimated attrition). A perfect fit would be an R^2 of one.

$$\boldsymbol{Objectivefunction} = \frac{1}{n}\sum_{i=1}^{n}\left(x_{i+1} - \left(\widehat{x_n} - a\frac{1}{d}\left(\widehat{y_n^p}\widehat{x_n^q}\right)h\right)\right)^2 + \left(y_{n+1} - \left(\widehat{y_n} - bd\left(\widehat{x_n^p}\widehat{y_n^q}\right)h\right)\right)^2 \quad (3)$$

2.2. EXPERT BLOCK

The development of decision-making is characterized by using intelligence resources through the predictive block and its interpretation, leading to the strategy definition. Once the global situation informed by the predictive block has been evaluated, it is necessary to redefine the strategy when there is a change of trend or when such trend change is sought by modifying the strategy (Defensive, Offensive, Stability, etc.). If the previous operational decisions are within the acceptable limits of attrition defined at the set point, the re-evaluation will not make sense in the first approximation.

The assessment of the adversary's intentions, strategy definition core, will be based on the actual ability to reject a possible attack in a hostile scenario. The contenders will consider a stable state situation if the probability of a failed attack exceeds the security level. The intention of an opponent to attack will be given by the minimum probability of success that the opponent needs to launch an attack **P** (this figure depends on the doctrine of the contender) and by the probability of being rejected by the defender, **WinsDef** curve (Equations 6 to 9). See literature sources [28,29].

$$\text{WinsDef} = \frac{1}{1+e^{0.12-3.38v}} \quad (6) \qquad v = \ln\sqrt{\frac{\delta}{\alpha}} \quad (7) \qquad \alpha = b\left(\frac{x_0}{y_0}\right) \quad (8) \qquad \delta = a\left(\frac{y_0}{x}\right) \quad (9)$$

2.3. SCHEDULER BLOCK

The COA planning is determined by military doctrine and the different factors of the operational environment, such as, for example, the enemy centers of gravity (COGs). Within the military decision-making process, the planning phase involves COA analysis, comparison, and evaluation, as well as the development of the matrix plan that provides the resources and conditions to optimize and maximize the results.

Action planning is inferred through decision trees, which process the doctrinal knowledge (friend and enemy), the strategy defined from the expert block, and evaluate possible outcomes in the context of probable enemy actions obtained through the predictive block.

The assessment of the alternatives is based on the concept of expected value E(x), applicable to random variables that take numerical values, and the utility of the COA. The final objective of the selected COA will be the fulfillment of the mission defined at the set point. In the current battle decisions, the own casualties x in combat is the main conditioning factor, so the Wald or pessimistic criterion is taken: it is a question of assuring conservative casualties (MAX MIN), Equation 4. This criterion involves selecting an alternative whose expected or average attrition is lower.

$$\mathrm{COAi} = \min(\mathrm{E}(\mathrm{x})) \quad (4)$$

2.3.1. CENTERS OF GRAVITY

All aspects of planning depend on the determination of well-defined, achievable, and measurable objectives. The process of identifying and defining objectives involves knowing the enemy, geography, and climate of the area of responsibility.

The objective acquisition model will be simplified using the K-Means clustering method (by the tactical disposition of the units in the terrain, using the Euclidean distance as a quantitative variable), obtaining the centers of concentration of the deployed units.

K-Means works by finding clusters with a spherical or convex shape and needs as input data the number of groups in which we are going to segment the population into k cluster, Elbow method, the algorithm according to [27], iterates with different values from 1 to n in the sense of reduction of the total sum of intracluster variance. Therefore, for each iteration, it takes the Euclidean distance between each unit with its center and adds up all the squares of the differences calculated (SSE), up to find the elbow point, where the SSE vs. cluster curve rate of decline is sharpened.

2.4. ADAPTIVE BLOCK

Even if a good battle model is available, changes in combat dynamics will lead to the deterioration of the model's fit (prediction and driving). The framework adapts to varying circumstances in the theater of operations and generates changes in the parameters that reflect the decisions' prediction and conditioning. Thus, adaptive control provides a solution theoretically capable of approximating the dynamics of the battle.

The adapting mechanism involves the following tasks:

- Adapting the prediction and factors that determine the strategy to the current battle situation.
- Setting the parameters of the COA usefulness.

This adapting mechanism is a learning process and will provide information for improving the model fit. The design of the adapting mechanism has focused on optimizing model prospect (i.e., on error minimization) and improving computational performance.

Figure 4 shows the adaptive predictive control scheme for practical application and implementation. The set point determines the criterion, on which the control acts by generating a feasible COA to change the negative trend.

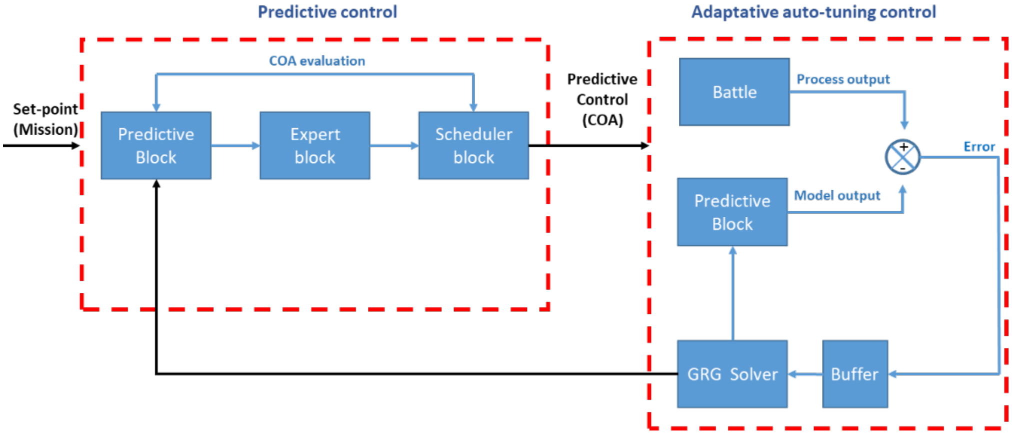


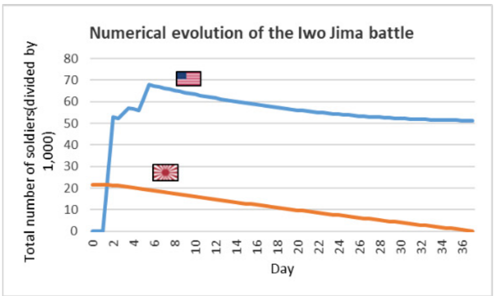
Figure 4. The adaptive control mechanism makes the discrepancy between the battle process output and the predictive model outputs tend to zero, highlighting the dual role played by the predictive block in the system at each sampling time window.

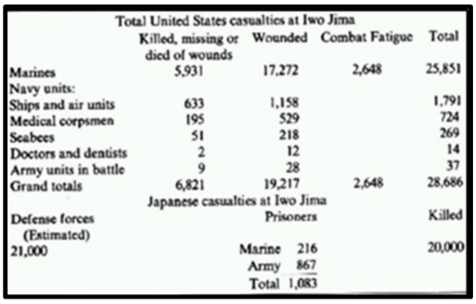
A supervised learning mechanism is used for the expert block adaptation, which extends the binary values (final result) of previous battles and recalculates the logistic regression base of the intention model, **WinsDef** curve. Adaptation is carried out after the final outcome.

3. EMPIRICAL VALIDATION

This framework was validated on three of the greatest battles of the Second World War, Creta, Iwo Jima, and Kursk battle. In these battles, the type of combat was mainly land-based. As this mode of combat has not essentially changed since then, the experimental results should be extrapolated adequately to present-day combat, e.g., the Bakhmut battle of the Russian invasion of Ukraine (2022).

In particular, on the Battle of Creta and Iwo Jima, our validation goal was to identify the best possible courses of action according to current doctrine and determine the effects they produce on the adversary in comparison with the actual battle on 20 May 1941 and 19 February 1945, on the Kursk battle, our goal was the correct identification of the battle phases by dynamically adjust from adaptive and predictive control. See literature sources [28,29].





Total United States casualties at Iwo Jima

	Killed, missing or died of wounds	Wounded	Combat Fatigue	Total
Marines	5,931	17,272	2,648	25,851
Navy units:				
Ships and air units	633	1,158		1,791
Medical corpsmen	195	529		724
Seabees	51	218		269
Doctors and dentists	2	12		14
Army units in battle	9	28		37
Grand totals	6,821	19,217	2,648	28,686

Japanese casualties at Iwo Jima

Defense forces (Estimated)	Prisoners	Killed
21,000	Marine 216 Army 867 Total 1,083	20,000

Figure 5: Example of performance of the framework on the evolution of the battle of Iwo Jima. The framework is able to replicate the actual dynamics of the battle that took place on February 19, 1945 [30,31].

Following science's good practices, the different software artifacts associated with the empirical validations are available publicly at this GitHub repository: https://github.com/gminguela/the-empirical-validation-of-the-framework-on-the-Battle-of-Crete-Iwo-Jima-and-Kursk-and-others

4. CONCLUSIONS

Due to the complexity of the military background, it is essential to make research advances and development efforts to enable decision automation, thus increasing the ability to anticipate the consequences of the adversary's possible actions and counteractions by new approaches and techniques that support the decision-making and the assessment under uncertainty. This presents a challenge for the upcoming battlefield, where the sophistication and scale of operations are expected to exceed the command's largely manual decision assessment capability.

Lanchester's classic work on battle dynamics modeling has inspired important research on the development of combat abstractions to support military decision-making under conditions of uncertainty, pursuing ways to achieve combat superiority. Nevertheless, it has been subject to the following criticisms: (a) it does not provide a fitting good enough for historical battle data, (b) it uses a constant lethality factor, (c) it deals with large battles with multiple types and phases as a whole, (d) it performs an oversimplistic one-sided treatment without taking into account opponent's capabilities, and (e) it cannot be used for disaggregated engagements.

To face those criticisms and overcome the current state, this paper has proposed a model that is focused on the types of decisions supported, how these types of decisions were made, and understanding the battle as a cause-effect process that evolves subject to changes and external actions.

Thus, our framework removes the limitations of Lanchester's classic work by dynamically adjusting the factors that define the evolution of the land battlefield, including learning mechanisms that optimize the capabilities of the architecture and, in short, the ability to improve decisions under uncertainty.

Currently, our framework assumes that the cause-effect relationship of the battle is modeled. However, there may be a chaotic behavior in the final phases that makes such modeling difficult in some battles. We plan as future work to apply Agent-Based Models (ABM) to overcome this problem.

References

1. Lanchester, F.W. Aircraft in Warfare: the Dawn of the Fourth Arm; Lanchester Press Inc.: Sunnyvale, CA, USA, 1916.

2. Christian, J.T. An Examination of Force Ratios; US Army Command and General Staff College Fort Leavenworth United States: Leavenworth, KS, USA, 2019.

3. Shlapak, D.A.; Orletsky, D.T.; Reid, T.I.; Tanner, M.R.;Wilson, B. A Question of Balance: Political Context and Military Aspects of the China-Taiwan Dispute; RAND Corporation: Santa Monica, CA, USA, 2009.

4. Shlapak, D.A.; Johnson, M. Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics; RR-1253-A; RAND Corporation: Santa Monica, CA, USA, 2016.

5. Chan, L.N.P. The Lanchester Square Law: Its Implications for Force Structure and Force Preparation of Singapore's Operationally Ready Soldiers. J. Singap. Armed Forces 2016, 42, 47–60.

6. Minguela-Castro, Gerardo, Ruben Heradio, and Carlos Cerrada. "Automated Support for Battle Decision Making: A Systematic Literature Review." (2022).

7. Kress, M.; Lin, K.Y.; MacKay, N.J. The attrition dynamics of multilateral war. Oper. Res. 2018, 66, 950–956. [https://pubsonline.informs.org/doi/10.1287/opre.2018.1718.

8. Chen, H.M. An optimal control problem in determining the optimal reinforcement schedules for the Lanchester equations. Comput. Oper. Res. 2003, 30, 1051–1066. [https://www.sciencedirect.com/science/article/abs/pii/S0305054802000564?via%3Dihub].

9. Coulson, S.G. Lanchester modeling of intelligence in combat. IMA J. Manag. Math. 2019, 30, 149–164. [https://academic.oup.com/imaman/articleabstract/30/2/149/4816352?redirectedFrom=fulltext]

10. Kim, D.; Moon, H.; Park, D.; Shin, H. An efficient approximate solution for stochastic. J. Oper. Res. 2017, 68, 1470–1481. [https://www.tandfonline.com/doi/full/10.1057/s41274-016-0163-6]

11. Fan, J.; Ren, H.; Tian, C. An Analysis of Wargame Rules Simulation Based on Stochastic Lanchester Mod. In Proceedings of the International Conference on Network, Communication and Computing (ICNCC), Kunming, China,

8–10 December 2017.

12. Ormrod, D.; Turnbull, B. Attrition rates and maneuver in agent based simulation models. J. Def. Model. Simul. Appl. Methodol. Technol. 2017, 14, 257–272.

13. Ajitha, S.; Datta, A.; Kumar, T.V.S. Multi-Agent based Artificial War. In Proceedings of the International Conference on Advanced Computing (ICoAC), Chennai, India, 14–16 December 2017.

14. Duffey, R.B. Dynamic theory of losses in wars and conflicts. Eur. J. Oper. Res. 2017, 261, 1013–1027. [https://www.sciencedirect.com/science/article/abs/pii/S0377221717302679?via%3Dihub].

15. Kress, M.; Caulkins, J.P.; Feichtinger, G.; Grass, D.; Seidl, A. Lanchester model for three-way combat. Eur. J. Oper. Res. 2018, 264, 46–54. [https://www.sciencedirect.com/science/article/abs/pii/S0377221717306537?via%3Dihub]

16. Epstein, J.M. The Calculus of ConventionalWar: Dynamic Analysis without Lanchester Theory; Brookings Institution Press: Washington, DC, USA, 1985.

17. Sanchez, J.M.; Rodellar, J. Adaptive Predictive Control: From the Concepts to Plant Optimization; Prentice Hall: Hoboken, NJ, USA, 1996.

18. F. W. Lanchester. Aircraft in Warfare: the Dawn of the Fourth Arm. Lanchester Press Inc., 1916.

19. S. J. Deitchman. A Lanchester Model of Guerrilla Warfare. Operations research, 10(6):818–827, 1962.

20. R. H. Peterson. Letter to the editor – On the "logarithmic law" of attrition and its application to tank combat. Operations Research, 15:557–558, 1967.

21. J. Bracken. Lanchester models of the Ardennes campaign. Naval Research Logistics, 42(4):559–577, 1995.

22. D. S. Hartley and R. L. Helmbold. Validating Lanchester's square law and other attrition models. Naval Research Logistics, 42(4):609–633, 1995.

23. M. P.Wiper, L. I. Pettit, and K.D.S. Young. Bayesian inference for a lanchester type combat model. Naval Research Logistics, 47(7):541–558, 2000.

24. T. W. Lucas and J. A. Dinges. The effect of battle circumstances on fitting Lanchester equations to the battle of kursk. Military Operations Research, 9(2):17–30, 2004.

25. J. Abadie. The grg method for nonlinear programming. Design and implementation of optimization software, pages 335–362, 1978.

26. L. Lasdon, A. Waren, A. Jain, and M. Ratner. Design and testing of a generalized reduced gradient code for nonlinear programming. ACM transactions on mathematical software, 4(1):34–50, Mar 1, 1978.

27. P. Bholowalia and A. Kumar. Ebk-means: A clustering technique based on elbow method and k-means in wsn. International Journal of Computer Applications, 105(9), 2014.

28. Gerardo Minguela-Castro, Ruben Heradio, and Carlos Cerrada. Automated Support for Battle Operational-Strategic Decision-Making. Mathematics, 2021, 9(13), 1534. [https://doi.org/10.3390/math9131534].

29. Castro, Gerardo Minguela. Automated support for battle operational-strategic decision-making. Diss. UNED. Universidad Nacional de Educación a Distancia (España), 2021. [http://e-spacio.uned.es/fez/view/tesisuned:ED-Pg-IngSisCon-Gminguela].

30. J. H. Engel. A Verification of Lanchester's Law. Journal of the Operations Research Society of America, 2(2):163–171, 1954.

31. J. H. Alexander. Closing in: Marines in the seizure of Iwo Jima. History and Museums Division, Headquarters, US Marine Corps, 1994.

Author

GERARDO MINGUELA CASTRO holds a Ph.D. in Control and System Engineering, a MS in Electric and Computer Engineering, and an MS Industrial Engineering degree from the National Distance University of Spain.

Mr. Minguela is Head of Public Sector Modernization Area at Isdefe (Isdefe is a public Spanish company that was created to provide technical engineering support and consulting services in advanced technologies in the defense sector) and his technical career has been devoted to tactical-level simulators design and development, complex system engineering, digital transformation, and software engineering. He was a member of the NATO Modeling and Simulation Group Technical Activity Programs MSG-027 ``Pathfinder'', SCRUM alliance, and SISO - Simulation Interoperability Standards Organization.

TOWARDS A NEW SYMBOLOGY AND VISUAL INTERACTION DESIGN FOR SUB-SEA MILITARY OPERATIONS

G. Walsh[1], N. S. Andersen[1], N. Stoianov[2] and S. J änicke[1]

Abstract

In a recently published survey on visual interfaces used in military decision support systems, we identified significant gaps in implementing best practice visualization techniques. These include the unmet use of alternative micro-visualizations which take into account the domain specific requirements of military support systems. We believe this lost opportunity results from NATO military standards which do not currently account for the novel types of user interactions required to carry out certain bespoke military operations. In particular, current military standards and products, fail to appropriately consider instances where user responses at a tactical level are limited, and must be brief, non-verbal, yet still enable succinct bi-directional communication between command and tactical forces. While many such gaps exist, for the purposes of this paper we restrict our focus to examining the possibility of a new sub-sea symbology for the maritime domain, based on knowledge we developed in the EDIDP project CUIIS (Comprehensive Underwater Intervention Information System). This paper proposes extending existing NATO military standards with the creation of a comprehensive proposal for a new Sub-sea symbology and visual interaction design framework for sub-sea military operations (SSMOs). The proposed framework includes a set of semiotic communication symbols for military divers which can easily be combined based on the most common messages required for effective communication between command and military divers.

Keywords

Human computer interaction (HCI); Interaction design; Visualization application domains; Visualization design and evaluation methods; • Applied computing → Military

1. INTRODUCTION

We recently published a survey [18], which analyzed twenty military command and control systems as well as integrated information systems through the creation of a domain-specific design space, identified gaps, opportunities and guidelines for improving the implementation of best practice visualization techniques. In particular our analyze found many of the surveyed military products fail to give appropriate forethought to domain-specific considerations such as environmental constraints, display and input constraints, as well as the suitable utilization of a comprehensive graphic design language [18]. Such identified failures in military products, are particularly prevalent in bespoke military operations, where tactical user requirements require customized software solutions.

1.1. ENVIRONMENTAL CONSTRAINTS OF THE SUB-SEA ENVIRONMENT

The different environmental conditions in which military operations take place result in stringent limits placed on military equipment capabilities [5]. These limits arise from demanding hardware requirements that downstream affect visual user interface (VUI) design possibilities and decisions [18]. Therefore, to strive for optimal end-user usability of the VUI of military decision-support systems, the assessment of visual interaction design factors such as i) Display Readability, ii) Display Fatigue, and iii) External Environmental factors should be considered according

[1] Department of Mathematics and Computer Science, University of Southern Denmark, Odense, Denmark {gwalsh, sindlev, stjaenicke}@imada.sdu.dk

[2] Department of Computing, Bulgarian Defence Institute, Sofia, Bulgaria n.stoianov@di.mod.bg

to the distinct environmental settings in which the system is utilized.

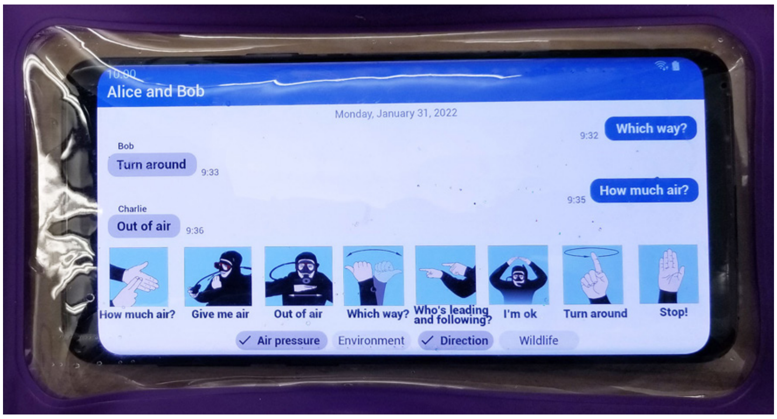
The sub-sea environment, in particular, imposes such a set of stringent limits of military equipment capabilities affecting end-user interaction with the VUI [17]. The constraints include the ability to successfully handle extreme weather conditions, where visibility may be dramatically reduced in, e.g., murky water and/or rough seas, functionality in an extreme range of temperatures, and the requirement of VUIs to account for visual distortion [10].

1.2. DISPLAY & INPUT CONSTRAINTS OF THE SUB-SEA ENVIRONMENT

Micro-displays are usually very small, ranging from around two to ten inches, with Tactical forces "on the ground" typically using such devices to display limited but vital information to tactical forces [18]. As the screen size of these displays is limited, so are the types and amount of visual information they can communicate to the end-user.

In sub-sea conditions, such displays are utilized in the form of dive computers or small tablet-like devices. However, a number of environmental display and input constraints unique to the sub-sea environment make commonly used information transferral and visualization techniques unsuitable. Such constraints affecting visual interaction with the VUI include; low-bandwidth transfer capability to the command and control system at the surface, touchscreens that are required to be resistant to salient water results in touchscreens that are bulky, less accurate, and less precise due to strict military standards that, e.g., enforce shock (MIL-S-901D) and vibration resistance (MIL-STD-167) [18]. Similarly, visual interaction with sub-sea VUIs should account for the perceived enlargement of objects to ensure usability is optimal and not affected.

The scoping review presented in [3] examines the capabilities of wearable devices for general underwater use. At the same time, some studies examine general visual interaction in the context of aquatic experience systems [4, 6, 7]. Yet, no existing research focuses on the capabilities and features of underwater devices specifically for military sub-sea purposes, and within the bespoke constraints such devices must operate within. In particular, there is a gap in the research arguing for the use of a new comprehensive semiotic visual interaction system to support Sub-Sea Military Operations (SSMOs). Such a system could operate in tandem with the devices on the surface at a command level, as well as with smaller devices in sub-sea conditions at a tactical level. A new visual interaction system with the versatility and robustness to operate similarly across head-mounted devices [9, 16], Augmented Reality (AR) displays [11, 2] among others, offers the possibility for increased technical innovation, integration, and most importantly could improve communication between military forces and command during SSMOs. For example, this could be achieved through the increased use of diver-tracking in terms of location [8, 14], depth, and diver status using appropriate and relevant NATO military symbology [13].



10:00

Alice and Bob

Monday, January 31, 2022

9:32 Which way?

Bob

Turn around 9:33

9:35 How much air?

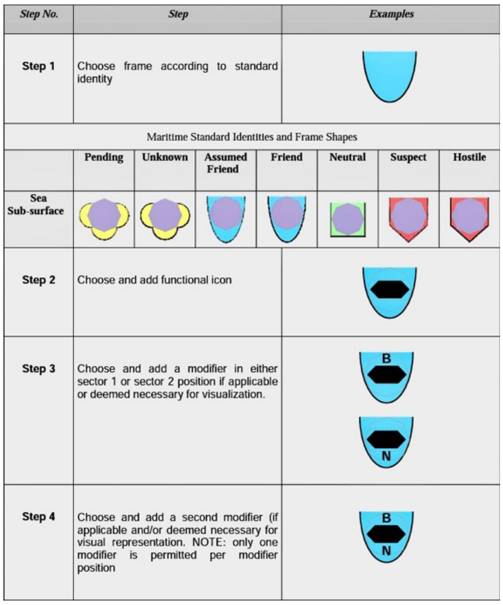
Charlie

Out of air 9:36

Figure 1: Image illustrating a novel communication method in terms of visual interaction for underwater civilian divers, which utilizes a small number of diver hand-signal images as easily selected statuses and messages to be communicated. Source:[4]

1.3. INTRODUCTION TO NATO SYMBOLOGY STANDARDS

One of the hindrances to the development of a comprehensive semiotic visual interaction system to support SSMOs is the strict requirement for graphical interfaces implemented in military software products to comply with NATO military symbology [13]. These symbology standards provide a standardized, structured set of graphical symbols for the display of information in command and control (C2) systems and applications. As shown in Figure 2, the symbology standard allows for a methodical process for symbol construction using building block elements such as i) Standard Identify, ii) Functional Icon, iii) Modifier, and iv) Second Modifier.



Step No.	Step	Examples
Step 1	Choose frame according to standard identity	

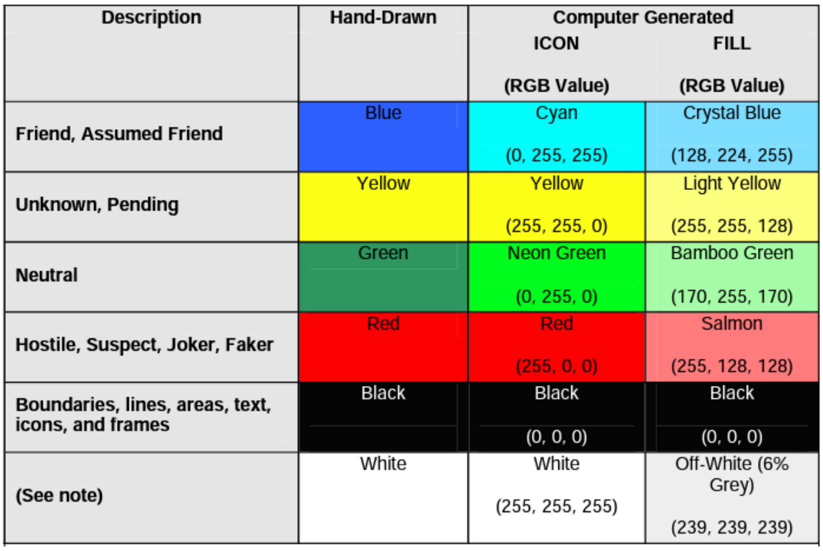
Maritime Standard Identities and Frame Shapes

	Pending	Unknown	Assumed Friend	Friend	Neutral	Suspect	Hostile
Sea Sub-surface							

Step No.	Step	Examples
Step 2	Choose and add functional icon	
Step 3	Choose and add a modifier in either sector 1 or sector 2 position if applicable or deemed necessary for visualization.	B N
Step 4	Choose and add a second modifier (if applicable and/or deemed necessary for visual representation. NOTE: only one modifier is permitted per modifier position	B N

Figure 2: Exert from NATO Military Symbology Standard APP-6(D) illustrating the construction of sub-sea representative icons based on a 4-step process including selection of Standard Identify, Functional Icon, Modifier, and Second Modifier as deemed suitable. Source: [13].

While the current standard allows for the creation of some new symbols, which may be needed in the future, certain elements in the standard, particularly those for the sub-sea environment, are outdated. A comprehensive symbol set and visual interaction design are lacking here, which can delineate the different types of divers, modern devices, and entities relevant to military sub-sea operations. The absence of a comprehensive symbology and visual interaction design standard is leading to poor uptake and adoption of NATO symbology standards in VUIs catering to such SSMOs. This results in a fragmented and ad-hoc representation of the different types of divers, modern devices, and entities relevant to military sub-sea operations across the software and devices currently being used. This is the very concern the NATO symbology standard sets out to mitigate and avoid. To address these concerns, further examination is required of the challenges faced by the current standard, as well as the task of framing the need for a new comprehensive symbology and visual interaction design for SSMOs.



Description	Hand-Drawn	Computer Generated ICON (RGB Value)	 FILL (RGB Value)
Friend, Assumed Friend	Blue	Cyan (0, 255, 255)	Crystal Blue (128, 224, 255)
Unknown, Pending	Yellow	Yellow (255, 255, 0)	Light Yellow (255, 255, 128)
Neutral	Green	Neon Green (0, 255, 0)	Bamboo Green (170, 255, 170)
Hostile, Suspect, Joker, Faker	Red	Red (255, 0, 0)	Salmon (255, 128, 128)
Boundaries, lines, areas, text, icons, and frames	Black	Black (0, 0, 0)	Black (0, 0, 0)
(See note)	White	White (255, 255, 255)	Off-White (6% Grey) (239, 239, 239)

Figure 3: Exert from NATO Military Symbology Standard APP-6(D) illustrating the description and corresponding distinct meaning of colors used in accordance with the standard which are handdrawn and computer generated. Source: [13]

2. CURRENT STATE OF SUB-SEA SYMBOLOGY & VISUAL INTERACTION IMPLEMENTATION

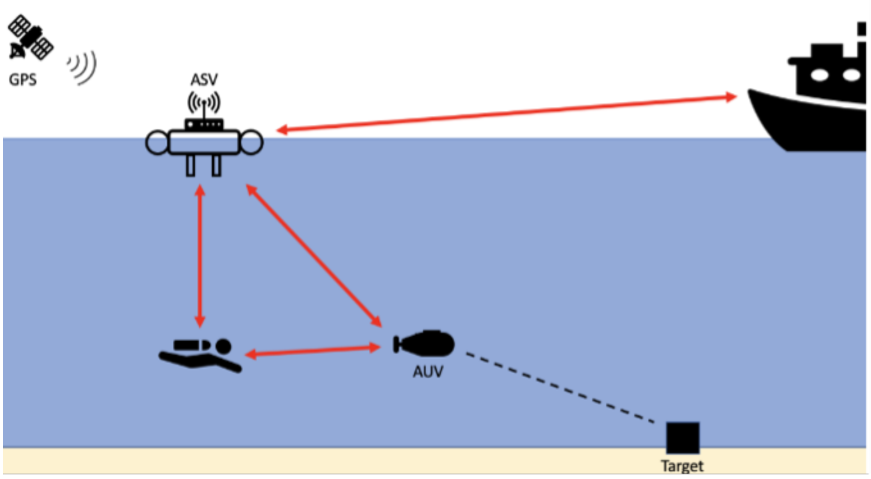


Figure 4: Illustration demonstrating the system architecture of software applications used to support SSMOs at a strategic level (above the surface) and at a tactical level (below the surface) with the integration of autonomous surface vehicles (ASVs) and autonomous underwater vehicles (AUVs). Source: [Wal]

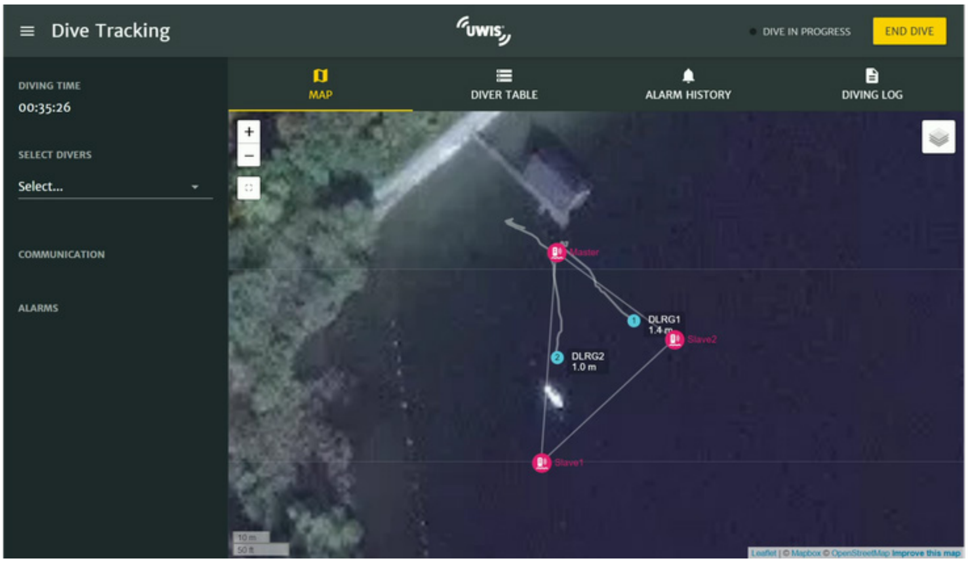
Sub-Sea Symbology and Visual Interaction Implementation needs to be designed to operate as two levels as shown in Figure 4, i) at a Command Level, which typically utilizes a desktop display at surface level, and ii) at a Tactical Level, which typically involves small screen wearable devices or tablets used in sub-sea conditions.

2.1. VISUAL INTERACTION AT A STRATEGIC LEVEL

Visualization at a strategic level in SSMOs, is primarily concerned with the representation of divers, and assets most commonly on a 2D cartographic map during the planning, execution and assessment phase of operations [18, 15]. Thus it is vital, to clearly identify the various actors encountered during an operation as well as their identity and function as shown in Figure 3, at a specified instance in space and time. Currently many software products in the sub-sea domain do not implement existing military symbology relating to sub-sea conditions. This has arisen because of the failure to update symbology standards in line with modern developments in military diving equipment, manned-unmanned teaming and modern sub-sea weapons as shown in Figure 7. Similarly, there is insufficient guidance in terms of how to incorporate symbology into directional markers, and the specific color values and graphic techniques which may be used to do so. This lack of comprehensive guidance for incorporating certain attributes into existing symbology also exists in the area of visualizing the trajectory, altitude, sensory data, and current status of actors and assets.

2.2. VISUAL INTERACTION AT A TACTICAL LEVEL

Visualization, at a tactical level in SSMOs, is constrained by the extreme environmental factors we mentioned earlier in subsection 1.2, resulting in display devices that are typically very small, ranging from a small dive computer to tablet-sized devices. Communication to the command at the surface is also limited, due to the limited applicable interaction methods possible, partly due to low bandwidth capabilities underwater, impracticality of verbal communication, and limited input of such touchscreens. As such, a greater emphasis is placed on information that can be easily communicated bidirectionally, briefly, succinctly, and using low bandwidth. Such methods of using predefined messaging for communication purposes underwater has been researched by [4] and is shown in Figure 1 in a civilian context. No research has been conducted on applying similar visual interaction and symbology techniques to be used in a military context.



DIVING TIME 00:35:26

SELECT DIVERS Select...

Figure 5: Screenshot from UWIS desktop software application illustrating how a dive may be currently represented on a map, with the representation of divers, buoys and the route which the diver has already travelled. Source: [1].

3. A NEW SYMBOLOGY & VISUAL INTERACTION DESIGN FOR SUB-SEA MILITARY OPERATIONS

The issues which are prevalent in the current implementation of sub-sea military symbology call for a complete revision, not only because they are limited and ambiguous, also, because of the lack of utilizing them in visual interfaces designed to support SSMOs.

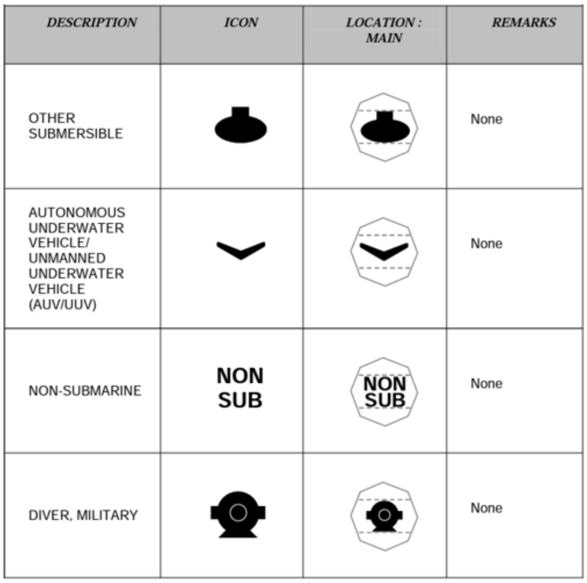
To date, these interfaces [18] have been developed without satisfying general visualization guidelines [12]. A comprehensive VUI for SSMOs must meet the following requirements:

- Revision of existing sub-sea military functional icons
- Design of new functional icons allowing to distinguish diver and UAV types
- Guidelines to use these symbols in/as pre-formatted messages

- Guidelines to use these symbols as directional markers
- Design to accurately represent altitude of actors and assets
- Representation of sensory data of actors and assets, most importantly, a comprehensive visual design to inform on the medical conditions of divers below the surface on small screens and above the surface on large screens
- Visual design for trajectory data of actors and assets
- Color mapping guidelines to accurately represent the given data in different visibility conditions

We argue the case for a number of modest, yet achievable and implementable revisions to current NATO Military Sub-Sea Symbology (APP-6D) to create a basis for a new symbology and visual interaction design for SSMOs. Advancements of such standards could enable the standardised development of a more user-friendly and cognitively efficient VUIs, as well as improve the communication interaction design between users at a command level and users at a tactical level throughout the planning, execution and assessment phase of operations.

We are currently developing an interactive front-end prototype of the command and control desktop application (over the surface) using the described new symbology and visual interaction design as part of our work on the CUIIS project. Our proposed design is illustrated in Figure 8. Its major component is a geospatial-temporal view that tracks divers, displaying their altitude as well as their medical conditions. We will evaluate the effectiveness and appropriateness of our functional prototype with military divers, marine commanders and NATO policy makers associated to the CUIIS project, ensuring to meet the needs of the military forces while complying to existing and further developing new NATO standards.



DESCRIPTION	ICON	LOCATION : MAIN	REMARKS
OTHER SUBMERSIBLE			None
AUTONOMOUS UNDERWATER VEHICLE/ UNMANNED UNDERWATER VEHICLE (AUV/UUV)			None
NON-SUBMARINE	NON SUB	NON SUB	None
DIVER, MILITARY			None

Figure 7: Exert from NATO Military Symbology Standard APP-6(D) illustrating the functional icons associated military sub-sea conditions. Visible in this exert is the outdated and ambiguous the functional icons. For example, the military diver icon is unclear whether it related to a diver which is tethered or untethered and can be easily misunderstood. Source: [13].

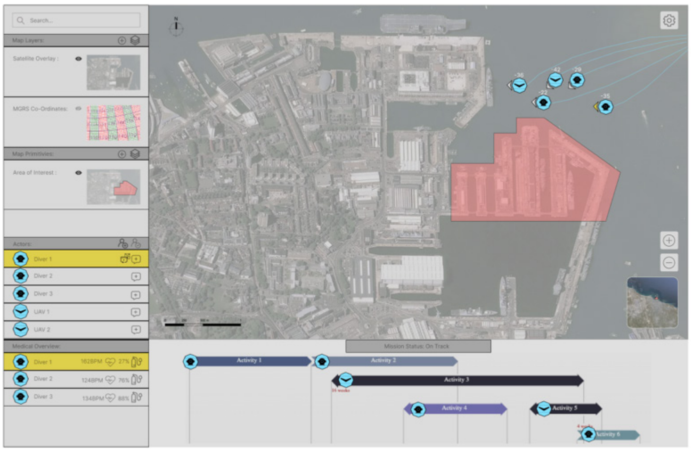


Figure 8: Illustration depicting how a New Comprehensive Symbology and Visual Interaction Design for Sub-Sea Military Operations could aid the development of VUI of software applications supporting such operations.

4. CONCLUSION

The current gap that exists between implementing best practices in terms of visualization and visual interaction in SSMOs occurs in part due to NATO military symbology standards, which are not fit for purpose for the sub-sea environment for use both at a command and tactical level in military software applications. We argue that the current gap can easily be closed by creating a revised NATO symbology standard, which creates a common and standardized new symbology and visual interaction design for SSMOs. Such a revision includes a set of semiotic communication symbols which can easily be combined based on the most common messages required for effective communication between command and military divers, as well as updated functional icons for divers, AUVs, directional markers, and additional guidance for representing altitude, sensory data and trajectory data. Implementation of a revised standard would standardize display of such VUI information across many sub-sea information systems which comply with military standards. In doing so, implementation of this new symbology and new visual interaction design for SSMOs will increase display readability, display fatigue, and be more appropriately tailored to the sub-sea environment. This in turn will increase forces at a strategic and a tactical level's ability to act, situational awareness, and decision-making ability.

5. ACKNOWLEDGEMENTS

Some images in the paper are included under the fair use copyright principle, which allows for the free use of portions of copyrighted materials for the purposes of commentary and discussion. Images courtesy of [4, 13, 1, 2].

The European Defence Industrial Development Programme has supported this research under the project CUIIS† (Grant Agreement EDIDP-UCCRS-EDD-2020-059 — CUIIS). The authors are solely responsible for this work which does not represent the opinion of the European Commission. The European Commission is not responsible for any use that might be made of information contained in this paper.

References

[1] ARVONEN P.: A revolutionary and proven to work system for underwater tracking, navigation and communication. https://uwis.fi/en/. Accessed: 2023-03-21. 4, 5

[2] BRUNO F., BARBIERI L., MANGERUGA M., COZZA M., LAGUDI A., ˇCEJKA J., LIAROKAPIS F., SKARLATOS D.: Underwater augmented reality for improving the diving experience in submerged archaeological sites. Ocean Engineering 190 (2019), 106487. doi:10.1016/j.oceaneng.2019.106487. 2, 4, 5

[3] BUBE B., ZANÓN B. B., LARA PALMA A. M., KLOCKE H.: Wearable devices in diving: Scoping review. JMIR mHealth and uHealth 10, 9 (2022), e35727. doi:10.2196/35727. 2

[4] CHEN T., CHAN J., GOLLAKOTA S.: Underwater messaging using mobile devices. In Proceedings of the ACM SIGCOMM 2022 Conference (New York, NY, USA, 2022), SIGCOMM '22, Association for Computing Machinery, p. 545–559. doi:10.1145/3544216.3544258. 2, 3, 5

[5] GARRETT III J. G.: The army and the environment: environmental considerations during army operations. International Law Studies 69,1 (1996), 37. 1

[6] GALLAGHER D. G., MANLEY R. J., HUGHES W. W., PILCHER A. M.: Divers augmented vision display (davd) emerging technology development. In OCEANS 2017-Anchorage (2017), IEEE, pp. 1–7. 2

[7] HATSUSHIKA D., NAGATA K., HASHIMOTO Y.: Scuba vr: Submersible-type virtual underwater experience system. In 2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR) (2019), IEEE, pp. 962–963. doi:10.1109/VR.2019.8798052. 2

[8] KUCH B., BUTTAZZO G., AZZOPARDI E., SAYER M., SIEBER A.: Gps diving computer for underwater tracking and mapping. Underwater Technology 30, 4 (2012), 189–194. doi:10.3723/ut.30.189. 2

[9] KOSS B., SIEBER A.: Head-mounted display for diving computer platform. Journal of Display Technology 7, 4 (2011), 193–199. doi:10.1109/JDT.2010.2103299. 2

[10] LURIA S. M., KINNEY J. A. S.: Underwater vision. Science 167, 3924 (1970), 1454–1461. doi:10.1126/science.167.3924.1454. 1

[11] MANLEY R. J., GALLAGHER D. G., HUGHES III W. W., PILCHER A. M.: Divers augmented vision display (davd). In ASME International Mechanical Engineering Congress and Exposition (2017), vol. 58493, American Society of Mechanical Engineers. doi:10.1115/IMECE2017-70026. 2

[12] MUNZNER T.: Visualization analysis and design. CRC press, 2014. 3

[13] NATO STANDARDIZATION OFFICE (NSO): Nato joint military symbology app-6(d). URL: https://litpolukrbrig.wp.mil.pl/u/APP-6D_JOINT_MILITARY_SYMBOLOGY._16_October_2017.pdf, 2019. Accessed: 2023-03-23. 2, 3, 5

[14] NAĐ , MANDI ´ C F., MIŠKOVI ´ C N.: Using autonomous underwater vehicles for diver tracking and navigation aiding. Journal of Marine Science and Engineering 8, 6 (2020), 413. doi:10.3390/jmse8060413. 2

[15] REILY T., BALESTRA M.: Applying Gestural Interfaces to Command-and-Control, vol. 6770 of DESIGN, USER EXPERIENCE, AND USABILITY: THEORY, METHODS, TOOLS AND PRACTICE, PT2. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, ch. 2, pp. 187–194. 3

[16] SIEBER A., KUCH B., ENOKSSON P., STOYANOVA-SIEBER M.: Development of a head-up displayed diving computer capability for full face masks. Underwater Technology 30, 4 (2012), 195–199. doi:10.3723/ut.30.195. 2

[17] SINEX C. H., WINOKUR R. S.: Environmental factors affecting military operations in the littoral battlespace. Johns Hopkins APL Technical Digest 14, 2 (1993), 112–124. 1

[18] WALSH G., ANDERSEN N. S., STOIANOV N., JÄNICKE S.: A survey of geospatial-temporal visualizations for military operations. In International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (2023), SCITEPRESS Digital Library, pp. 115–129. doi:10.5220/0011902500003417. 1, 2, 3

Author:

Gareth Walsh

Research lies at the intersection of visualization, user interface design and HCI, with a specific interest in developing novel geospatial-temporal visualizations and micro-visualizations for military command and control systems and integrated sub-sea tactical systems.

EUROPEAN
DEFENCE
AGENCY

LEAGUE OF ALGORITHMS: A NOVEL DATA AUGMENTATION APPROACH TO BUILD A TRAINING DATASET FOR IMAGE TO IMAGE TRANSLATION PROBLEMS

Niccolò Camarlinghi[1]1, Antonio Di Tommaso1, Benedetto Michelozzi1, Giacomo Fontanelli1, Andrea Masini1

Abstract

The lack of high-quality data is becoming a critical bottleneck for modern machine learning algorithms. In this paper, we proposed a novel data augmentation method that tackles some critical aspects often found in image-to-image translation problems. The proposed method is called League of Algorithms (LoA) and consists in applying an ensemble bagging using the outcome of several image-to-image algorithms to generate images that can be used as ground truth. LoA can be applied to any set of images to produce, virtually, an arbitrary-size dataset. In this paper, the capability of LoA is demonstrated through the "de-hazing" problem, which consists in removing the layer of fog/haze present in visually degraded scenarios. The results show that using the LoA generated dataset, it is possible to obtain results comparable o better with respect to standard data augmentation. Despite the fact that the LoA was applied only to dehazing we foresee possible applications to other problems in the image-to-image domain.

Keywords

Situational awareness, artificial intelligence, data augmentation, image-to-image translation

1. INTRODUCTION

Machine learning is becoming a widespread tool in many sectors with defense being no exception. One of the most common problems to face when dealing with machine learning concerns the availability of quality data for training and validation. In many cases, data can be obtained either by data collection, data synthesis, or data augmentation, i.e., performing various transformations to existing data points to improve model generalization and data cardinality. In this paper, we propose a novel data augmentation method, named League of Algorithms (LoA). This approach can be applied to image-to-image translation problems, i.e., problems where the goal is to obtain a mapping between two sets of images. This method allows to build, virtually, an arbitrary size training/validation dataset.

Constructing a LoA consists in:

1. Selecting a dataset
2. Building the league: Selecting a number of already developed and trained algorithms that solve the selected image-to-image problem.
3. Use each algorithm as a weak learner and applying an ensemble bagging to their output.

The output of the LoA is a set of images, that can be used as ground truth when performing a training/validation of the selected image to image task. In this paper we investigated the performance of the LoA in the context of "de-hazing", using an average fusion algorithm as bagging rule. Dehazing consists in restoring the degraded visibility caused by bad atmospheric conditions, such as mist and fog. To train a dehazing algorithm a set of clean/hazy pictures of the same hazy scene is needed. However, this problem is non-trivial and was tackled in different ways: Acquiring hazy/clean images of the same scene under different weather conditions [1], [2], applying data

[1] FlySight Srl, Via A. Lampredi 45, Livorno 57121, Italy. niccolo.camarlinghi@flysight.it, antonio.ditommaso@flysight.it, benedetto.michelozzi@flysight.it, giacomo.fontanelli@flysight.it, andrea.masini@flysight.it

augmentation to add a layer of synthetic haze to the clean images [2], [3], or using a fog machine to produce hazy/clean images corresponding to the same scene [4]–[6]. The Dataset generated using the acquisition of real data, generally, suffers from both limited data cardinality and poor correspondence between hazy and clean scene, on the other hand, dataset created by adding a synthetic layer of haze tends to be unrealistic especially when a thick layer of haze is applied. Moreover, haze augmentation often relies on knowing the scene depth map which is often non-available and has to be estimated through other algorithms such as [7]. Despite the method used, dehazing remains typically an ill-posed problem, as, in general, no exact mapping between the input and output image exists. For example, a very dense layer of haze could make the real information contained in the clean image impossible to recover.

In this paper, we built a dataset of hazy/clean images starting from an arbitrary set of pictures downloaded from flickr [8]. This approach tackles the following critical aspects:

- Dataset cardinality: this approach can be applied, virtually, to an arbitrary number of images to produce a dataset fitting the application need.
- Correspondence: As for others data augmentation methods, e.g., adding layer of synthetic haze to a scene, the correspondence between ground truth and clean images is obtained by design.
- Ill-posedness: The details contained in the "clean" images produced by the LoA are the result of processing the hazy image, this reduces the problem ill-posedness, as it makes the mapping between hazy and clean images theoretically achievable.

To show that LoA provides a good estimate of the clean images, we performed training using Enhanced Pix2pix Dehazing (EPDN) Network [9] and we compared the results with those obtained using the model provided by the original authors.

2. MATERIAL AND METHODS

2.1. LEAGUE OF ALGORIHTMS (LOA)

To build the LoA seven different publicly available dehazing models were used as weak learners: Dark Channel Prior [10], Non-Local Image Dehazing [11], CLAHE [12], DehazeFormer [13], Dehaze-GAN [14], Pix2Pix [15] and FFA-Net [16]. Dark channel prior and non-local image dehazing are two prior-based algorithms trying to recover the clean image by estimating the air-light and transmission map of the scene. CLAHE is a widely used restoration algorithm, whereas the DehazeFormer is a vision transformer specifically implemented for dehazing images. Dehaze-GAN and Pix2Pix are instead two Generative Adversarial Networks (GAN), meant to produce directly "clean" images. Since no pretrained models were publicly available for these latter two algorithms, we trained them from scratch using a synthetic haze dataset built from the make3D dataset [17]. To generate the ground truth of an image I using the LoA, each algorithm is first applied on I, to provide its output O_i, then an average image fusion is applied to produce the ground truth image $\mathrm{O}_{\mathrm{LoA}}$

$$\boldsymbol{O_{LoA}} = \frac{\sum_{i=1}^{N} \boldsymbol{O_i}}{\boldsymbol{N}}$$

where $\mathrm{N}=7$ for the case under study. Two examples of the ground truth images generated by the LoA are shown in *Figure 1* right column.

2.2. THE FLICKR DATASET

A dataset of 3000 pictures licensed as "available for commercial use" was downloaded from the flickr website, by using the keyword "mist". By discarding manually corrupted and other unsuitable images, e.g., images containing artistic effects, a set of 2364 images was obtained. The set consists of totally unrelated hazy urban and rural scenarios. The size of the images contained in the dataset ranged up to 20000 x 5000 pixels. We decided to rescale those images with a resolution higher than full HD (1920 x 1080) to full HD while zero padding to maintain the aspect ratio. An example of the downloaded image is show in *Figure 1*.

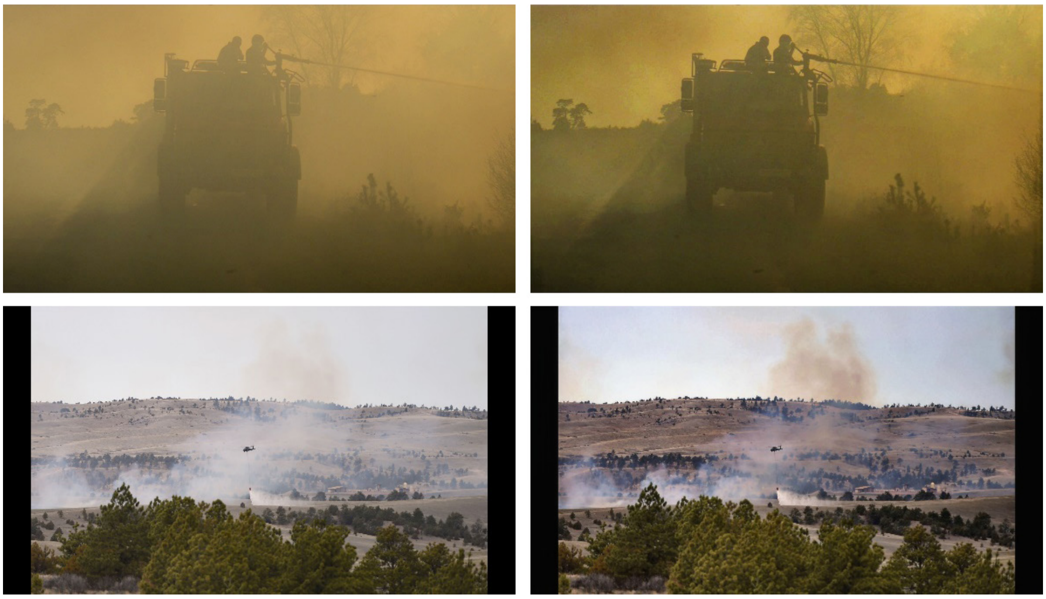


Figure 1: Left column: Two example images from flickr dataset. Right column the corresponding images generated by the LoA.

2.3. ENHANCED PIX2PIX DEHAZING ALGORITHM (EPDN)

EPDN was originally presented in [9] and features two GANs, acting at different scale levels, followed by two enhancing blocks. The model used in the original EPDN paper was obtained by training it on Indoor Training Set (ITS) RESIDE subset [2]. A custom EPDN model was trained for 200 epochs on the flickr dataset using the same settings described in [9]. The obtained model will be referred in the next sections as "Our".

2.4. VALIDATION SETS

Validation was performed on four public datasets: DENSE-HAZE [6], NH-HAZE[18], O-HAZE[4] and SOTS [2]. DENSE-HAZE, NH-HAZE and O-HAZE consists of images generated using a fog machine, with DENSE-HAZE including scenes with a very thick haze. SOTS dataset in turn is generated by performing haze augmentation on "clean" images belonging to the NYU2 dataset. Table 1 resumes some of the main characteristics of the datasets used in this study.

Table 1: Characteristics of the four datasets used in this study.

Dataset	Haze Type	Location	Cardinality
DENSE-HAZE	Fog machine	Indoor/Outdoor	22/33
NH-HAZE	Fog machine	Outdoor	55
O-HAZE	Fog machine	Outdoor	45
SOTS	Data augmented	Indoor/Outdoor	500/500

Evaluation of the performance of the original EPDN and the model trained using the dataset generated with LoA was performed using three "full reference" metrics, Structural Similarity Index Measure (SSIM) [19], Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE) and three "no reference" metrics, NIQE [20], PIQE [21], BRISQUE [22]. Table 2 describes some basic aspect of the used metrics.

Table 2: Basic aspects of the metrics used in this study.

	SSIM	PSNR	MSE	NIQE	PIQE	BRISQUE
Range	[-1,1]	[0,∞]	[0,∞]	[0,100]	[0,100]	[0,100]
Score meaning	Higher is better	Higher is better	Less is better	Less is better	Less is better	Less is better

2.5. RESULTS

The results of the evaluation of the original EPDN model and "Our" model are shown in Table 3 and Table 4. The results show that the newly trained model performs similarly or better with respect to the original model with the only exception being the SOTS indoor dataset. This discrepancy could be explained by the fact that "Our" model was trained on outdoor scenes only. Some examples of dehazed images from the four datasets considered for this study are shown in Figure 2. A visual inspection shows that "Our" model, tends to remove less haze, in particular in case of very thick haze, but at the same time, it restores, most of the times, colors closer to those of the original scene while maintaining more details in the background and providing a more natural looking scene. Moreover, we observed that "Our" model is less prone to produce artifacts in images (see Figure 3), this can be the result of reducing the degree of ill-posedeness of the problem.

Table 3 Results obtained on the four datasets of this study for "full reference" metrics. Green and red colored numbers correspond respectively to "Our" model outperforming/underperforming the original EPDN model

Dataset	Model	SSIM	PSNR	MSE
DENSE-HAZE	EPDN [9]	0.47	13.08	3680.93
	"Our"	0.47	13.25	3357.04
NH-HAZE	EPDN [9]	0.5	12.92	3683.13
	"Our"	0.49	13.3	3282.2
O-HAZE	EPDN [9]	0.64	16.65	1581.83
	"Our"	0.65	17.32	1359.09
SOTS indoor	EPDN [9]	0.91	25.01	264.54
	"Our"	0.84	20.36	746.49
SOTS outdoor	EPDN [9]	0.86	20.2	876.26
		0.89	21.06	635.17

Table 4 Results obtained on the four datasets of this study for "no reference" metrics. Green and red colored numbers correspond respectively to "Our" model outperforming/underperforming the original EPDN model.

Dataset	Model	NIQE	PIQE	BRISQUE
DENSE-HAZE	EPDN [9]	6.2	9.61	31
	"Our"	7.03	9.36	27.16
NH-HAZE	EPDN [9]	4.78	6.63	36.47
	"Our"	4.24	6.35	33.35
O-HAZE	EPDN [9]	6.44	20.07	39.07
	"Our"	5.75	21.17	36.45
SOTS indoor	EPDN [9]	7.29	37.72	40.67
	"Our"	7.05	39.8	40.68
SOTS outdoor	EPDN [9]	5.19	8.88	34.33
		4.8	10.64	36.35

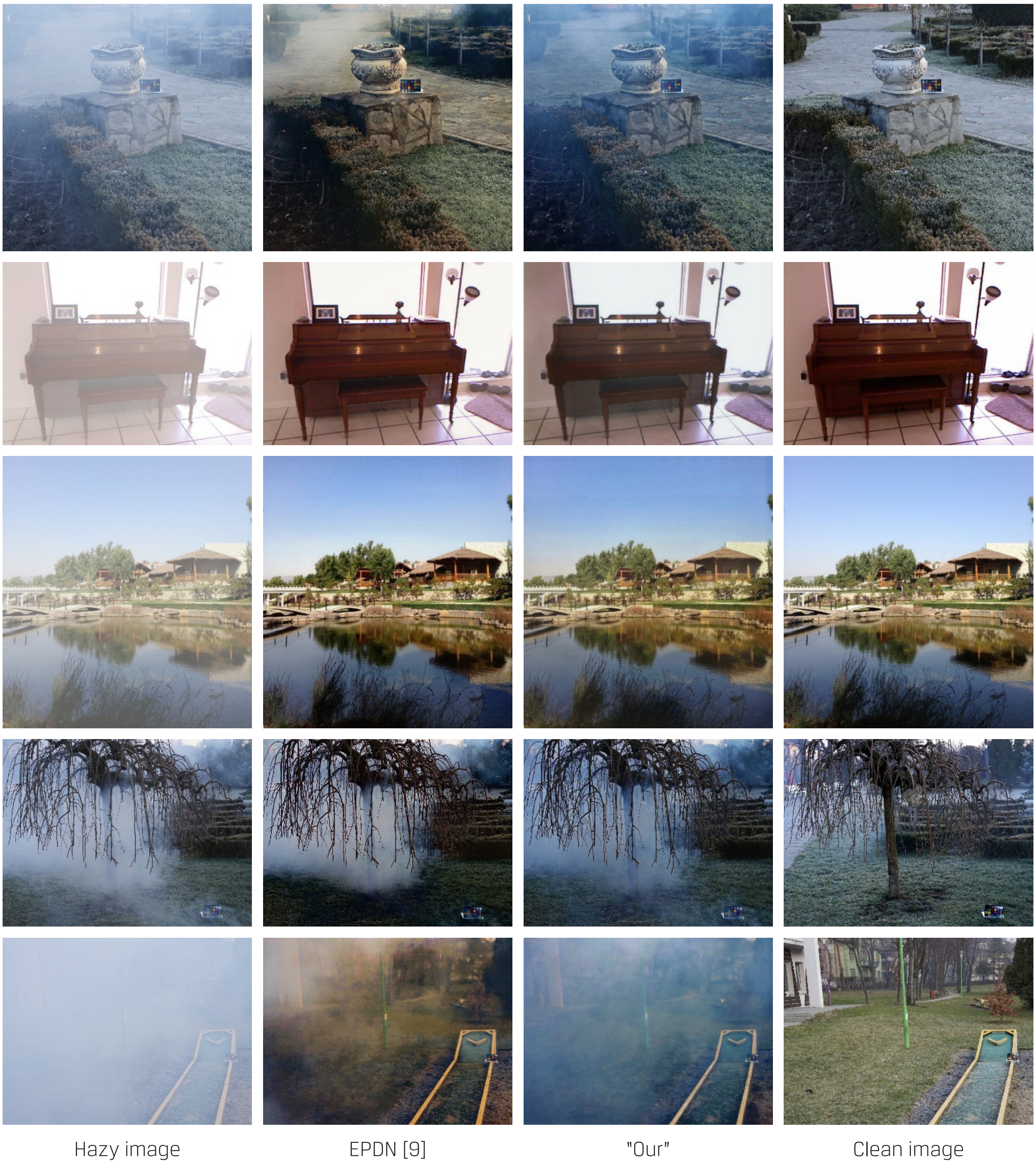


Figure 2: Comparison of visual effects produced by the original EPDN model and "Our" model. From top to bottom O-HAZE, SOTS indoor, SOTS outdoor, NH-HAZE and DENSE-HAZE.

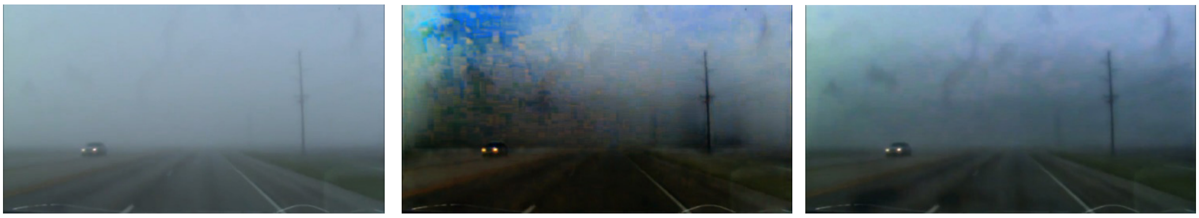


Figure 3: An image from RESIDE dataset (left), dehazing using EPDN (center) and dehazing with "Our" model (right).

2.6 CONCLUSION AND DISCUSSION

In this paper, we described a novel data augmentation method named League of Algorithms (LoA) that can be adapted to provide an estimation of ground truth for image-to-image translation problems. We have shown that, in the context of dehazing, this approach leads to results comparable to those obtainable using a standard augmentation approach. With respect to common augmentation approaches, the LoA is more computationally expensive as it requires to run each algorithm on the whole set of images. However, the bagging strategy make it robust and less prone to produce artifacts, therefore it suits well the creation of large dataset without the need for manual quality control of the generated images.

References

[1] W. Liu, F. Zhou, T. Lu, J. Duan, and G. Qiu, "Image Defogging Quality Assessment: Real-World Database and Method," IEEE Trans Image Process, vol. 30, pp. 176–190, 2021, doi: 10.1109/TIP.2020.3033402.

[2] B. Li et al., "Benchmarking Single Image Dehazing and Beyond." arXiv, Apr. 21, 2019. Accessed: Oct. 12, 2022. [Online]. Available: http://arxiv.org/abs/1712.04143

[3] Y. Zhang, L. Ding, and G. Sharma, "HazeRD: an outdoor scene dataset and benchmark for Single image dehazing," in Proc. IEEE Intl. Conf. Image Proc., Sep. 2017, pp. 3205–3209. doi: 10.1109/ICIP.2017.8296874.

[4] C. O. Ancuti, C. Ancuti, R. Timofte, and C. D. Vleeschouwer, "O-HAZE: a dehazing benchmark with real hazy and haze-free outdoor images," in IEEE Conference on Computer Vision and Pattern Recognition, NTIRE Workshop, in NTIRE CVPR'18. 2018.

[5] C. Ancuti, C. O. Ancuti, and C. De Vleeschouwer, "D-HAZY: A dataset to evaluate quantitatively dehazing algorithms," in 2016 IEEE International Conference on Image Processing (ICIP), Sep. 2016, pp. 2226–2230. doi: 10.1109/ICIP.2016.7532754.

[6] C. O. Ancuti, C. Ancuti, R. Timofte, L. V. Gool, L. Zhang, and M.-H. Yang, "NTIRE 2019 Image Dehazing Challenge Report," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, in IEEE CVPR 2019. 2019.

[7] Z. Li and N. Snavely, "MegaDepth: Learning Single-View Depth Prediction from Internet Photos." arXiv, Nov. 27, 2018. Accessed: Oct. 12, 2022. [Online]. Available: http://arxiv.org/abs/1804.00607

[8] "Flickr website." https://www.flickr.com/

[9] Y. Qu, Y. Chen, J. Huang, and Y. Xie, "Enhanced Pix2pix Dehazing Network," in 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Jun. 2019, pp. 8152–8160. doi: 10.1109/CVPR.2019.00835.

[10] K. He, J. Sun, and X. Tang, "Single Image Haze Removal Using Dark Channel Prior," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 12, pp. 2341–2353, Dec. 2011, doi: 10.1109/TPAMI.2010.168.

[11] D. Berman, T. Treibitz, and S. Avidan, "Non-Local Image Dehazing," presented at the Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2016, pp. 1674–1682. Accessed: Sep. 14, 2022. [Online]. Available: https://openaccess.thecvf.com/content_cvpr_2016/html/Berman_Non-Local_Image_Dehazing_CVPR_2016_paper.html

[12] S. S. Agaian, B. Silver, and K. A. Panetta, "Transform Coefficient Histogram-Based Image Enhancement Algorithms Using Contrast Entropy," IEEE Transactions on Image Processing, vol. 16, no. 3, pp. 741–758, Mar. 2007, doi: 10.1109/TIP.2006.888338.

[13] Y. Song, Z. He, H. Qian, and X. Du, "Vision Transformers for Single Image Dehazing," arXiv preprint arXiv:2204.03883, 2022.

[14] N. Bharath Raj and N. Venketeswaran, "Single Image Haze Removal using a Generative Adversarial Network," in 2020 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), Aug. 2020, pp. 37–42. doi: 10.1109/WiSPNET48689.2020.9198400.

[15] P. Isola, J.-Y. Zhu, T. Zhou, and A. A. Efros, "Image-To-Image Translation With Conditional Adversarial Networks," presented at the Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017, pp. 1125–1134. Accessed: Sep. 14, 2022. [Online]. Available: https://openaccess.thecvf.com/content_cvpr_2017/html/Isola_Image-To-Image_Translation_With_CVPR_2017_paper.html

[16] X. Qin, Z. Wang, Y. Bai, X. Xie, and H. Jia, "FFA-Net: Feature fusion attention network for single image dehazing," in Proceedings of the AAAI Conference on Artificial Intelligence, 2020, pp. 11908–11915.

[17] A. Saxena, M. Sun, and A. Y. Ng, "Make3D: Learning 3D Scene Structure from a Single Still Image," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 31, no. 5, pp. 824–840, May 2009, doi: 10.1109/TPAMI.2008.132.

[18] C. O. Ancuti, C. Ancuti, and R. Timofte, "NH-HAZE: An Image Dehazing Benchmark with Non-Homogeneous Hazy and Haze-Free Images," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, in IEEE CVPR 2020. 2020.

[19] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600–612, Apr. 2004, doi: 10.1109/TIP.2003.819861.

[20] A. Mittal, R. Soundararajan, and A. C. Bovik, "Making a 'Completely Blind' Image Quality Analyzer," IEEE Signal Processing Letters, vol. 20, no. 3, pp. 209–212, Mar. 2013, doi: 10.1109/LSP.2012.2227726.

[21] Venkatanath, M. C. Bh, S. S. Channappayya, and S. S. Medasani, "Blind image quality evaluation using perception based features," in 2015 Twenty First National Conference on Communications (NCC), Feb. 2015, pp. 1–6. doi: 10.1109/NCC.2015.7084843.

[22] A. Mittal, A. K. Moorthy, and A. C. Bovik, "No-Reference Image Quality Assessment in the Spatial Domain," IEEE Transactions on Image Processing, vol. 21, no. 12, pp. 4695–4708, Dec. 2012, doi: 10.1109/TIP.2012.2214050.

Authors

Niccolò Camarlinghi

Dr. Niccolò Camarlinghi received his Bachelor's Degree in general physics in 2004, his Master's Degree in theoretical physics in 2007, and his Ph.D. in Applied Physics in 2012 from Pisa University. He is now working at FlySight Srl, as head of research.

Antonio Di Tommaso

Antonio Di Tommaso is a data scientist and researcher for FlySight Srl with a passion for uncovering insights and driving innovation through data. He specializes in AI, with a particular focus on automatic target recognition and satellite image processing. Antonio earned his bachelor's and master's degrees in Computer Science and Data Science at the University of Pisa.

Benedetto Michelozzi

Dr. Benedetto Michelozzi received his master degree in Physics from the University of Pisa (Italy) in 1989. Currently he is the key person in the FlySight Srl R&D Team. His current research interests concern with the development of remote sensing HW/SW applications, acquisition/processing of neuromorphic cameras, Visible/IR/Multispectral/Hyperspectral images, data fusion and enhancement.

Giacomo Fontanelli

Dr. Giacomo Fontanelli got his master degree in "Information Engineering" from University of Pisa in 2013 and has been working in the field of multispectral remote sensing since, managing the development of integrated hardware/software solutions for innovative programs in the industrial sector. He was involved in several national and international research projects such as ASI co-funded ACAS project and the ESA co-funded "SP4GO", "Sun4Health", "i-FishSAT" projects.

Andrea Masini

Andrea Masini received his master degree in Telecommunications Engineering in 2004 from the University of Pisa. In 2020 he was the principal promoter for the foundation of FlySight Srl, a company entirely owned by Flyby group and devoted exclusively to the defense security and space sector and he took the role of CTO in this new company. In 2020 he has been elected Deputy Industrial Rapporteur of the EDA CapTech Optronics. In his career, Andrea has contributed to several NATO initiatives (NIAG SG 232, SG 249, SG 256, IST-168), and has been author and co-author of more than 30 scientific papers in journals and conference proceedings.

A MOBILE RADIATION DETECTION SYSTEM FOR SECURITY AND DEFENCE

Luís Miguel Cabeça Marques[1], Alberto Manuel Martinho Vale[2] and José Pedro Miragaia Trancoso Vaz[3]

Abstract

The detection, identification and localization of special nuclear materials and other radioactive materials or sources used in industry, medicine and research are of paramount importance due to their possible use on improvised nuclear devices and radiological dispersal or exposed devices respectively. To tackle against the illicit traffic of these materials, normally large and expensive fixed radiation detection systems are used on airports, maritime ports and land borders. This work presents a mobile radiation detection system based on plastic scintillators with silicon photomultiplier sensors for the detection and localization of gamma, beta and neutron sources/materials. Advantages as low cost, low weight, low consumption and high geometric efficiency allied to its integration on a highly maneuverable drone makes it the ideal tool for front-line officers or CBRNe response teams in the search of radioactive sources shielded or not (e.g. inspection of infrastructures) and mapping or monitoring of contaminated areas.

Keywords

Mobile radiation detection system, Unmanned aerial vehicle, Special nuclear materials, Silicon photomultipliers, Plastic scintillators.

1. INTRODUCTION

Effective measures to control and avoid unauthorized transfer of special nuclear materials (SNMs) and other radioactive materials, as well as equipment, technology, information that may be used to develop improvised nuclear devices (INDs) or radiological dispersal devices are necessary. While the use of SNMs (e.g. highly enriched uranium or plutonium) to development INDs could cause major casualties; the use of radioactive materials or sources normally used in medicine, industry and research can be used to develop weapons of massive disruption with enormous social and economic consequences such as radiological dispersal devices (RDD) or radiological exposure devices (RED). Another threat may be the dispersing of radioactive materials because of the sabotage or attack of a nuclear facility or during the radioactive material transportation [1]. Among many recommended measures of the International Atomic Energy Agency (IAEA) for a consistent nuclear security detection architecture is the development of radiation detection systems and measures, technologies and non-technological solutions to mitigate or eliminate such vulnerabilities [2].

In order to avoid the illicit traffic of SNMs and other radioactive materials normally fixed radiation portal monitors (RPMs) are used on airports, land borders and maritime ports. Portable RPMs can also be used to monitor vehicles or persons in major public events or in the aftermath of a radiological and nuclear emergency, however it normally needs to be disassembled and again mounted every time they need to change place. Fixed and portable RPMs are characterized by a high detection efficiency to gamma-rays and in some cases to neutrons (when available), achieved using large detection systems [3] [4]. However, the high acquisition, operational and maintenance costs of RPMs and their lack of mobility leads to some security issues: i) only some airports, land borders and maritime ports have RPMs; ii) only a small fraction of shipping containers are inspected on maritime ports, since transshipment

[1] Centro de Investigação da Academia da Força Aérea – Academia da Força Aérea, Pêro Pinheiro, Portugal
lumarques@academiafa.edu.pt

[2] Instituto de Plasmas e Fusão Nuclear – Instituto Superior Técnico, Lisboa, Portugal
avale@ipfn.tecnico.ulisboa.pt

[3] Centro de Ciências e Tecnologias Nucleares – Instituto Superior Técnico, Lisboa, Portugal
pedrovaz@ctn.tecnico.ulisboa.pt

cargo don´t pass through RPMs (generally placed at the entrance/exit of the ports). While primary inspections to shipping containers are performed with RPMs within one minute, secondary inspections (performed when a radioactive source triggers an alarm on a RPM) can take up to 20 minutes using handheld equipment [5].

The use of a neutron detection system as a complement of a gamma-ray detector is very important, since in Security and Defence applications it is necessary to detect neutron sources as 241Am-beryllium (Am-Be), 252Cf and SNMs, in particular plutonium. Despite Am-Be and plutonium being both a gamma-ray and neutron emitter, the low energy gamma-rays emitted and their possible shielding (with some cm of lead), makes the use of a neutron detector crucial for the detection of these threats. The most common neutron detection system is based on helium-3, however there is a worldwide shortage of this gas and it is necessary to find an alternative.

Mobile radiation detection systems can be an alternative or complement to RPMs. However, the need to detect weak sources (e.g. SNMs), shielded sources (by cargo or other material), and the significant source detector distances, leads to the use of large radiation detection systems carried by cars, trucks or trailers. In literature gamma radiation detection systems were also coupled to small unmanned aerial vehicles, such as: i) inorganic scintillators, e.g. NaI(Tl) and CsI(Tl)) with silicon photomultiplier sensors; ii) semiconductors, e.g. CdZnTe; iii) Gamma imagers. A dual-mode detector (able to detect both gamma-rays and neutrons) was also integrated in a multirotor. Despite these detection systems can simultaneously detect and identify the radionuclides, they are expensive, are only available in small crystals, and cannot handle high dose rates (normally a Geiger-Muller detector must also be used together to deal with high doses monitoring) [4].

In this paper a compact, lightweight and low power consumption mobile radiation detection system is described based on plastic scintillators with silicon photomultiplier sensors for the fast detection and localization of gamma, beta and neutron sources. Due to its independent power supply and global navigation satellite system (GNSS) antenna, the radiation detection system can be coupled to any mobile platform (ground, air or hybrid). The integration of the detection system on a highly maneuverable multirotor (drone) allowed to reduce the source detector distance and to use more compact detection systems. By performing lateral wall inspections to a shipping container, it was possible to detect a hidden 4 MBq 137Cs gamma-ray source and a 1.45 GBq Am-Be neutron source within 30 seconds (primary inspection). For gamma-ray source localization purposes complete turns were performed to the shipping container (2-3 minutes) obtaining a localization precision of approximately 1 m. The low cost, low power consumption and high detection efficiency of this radiation detection system facilitates its reproduction in several platforms aiming for faster and autonomous inspection/monitoring using unmanned vehicles.

2. MATERIALS AND METHODS

This chapter briefly describes the developed mobile radiation detection system and its architecture as well as the methods used to optimize the detection efficiency and to test it with real radioactive sources. A more detailed description of the radiation detection system can be found in [5] and [6].

2.1. MOBILE RADIATION DETECTION SYSTEM

The proposed detection system is based on plastic scintillators with SiPM sensors. The use of plastic scintillators presents several advantages, such as: low-cost material, fast response and are available in different shapes (e.g. pancake shape) and sizes. The SiPM sensors are used to convert the scintillation light produced inside the sensitive volume of the scintillators into electric signals which will be read and processed by a multichannel analyzer (MCA). Unlike traditional photomultiplier tubes (PMTs), SiPM sensors are more compact, lightweight, low power consumption and are immune to magnetic field interference. Therefore, the combination of plastic scintillators with SiPM sensors allows the best detection efficiency per weight.

The developed mobile radiation detection system (shown in Figure 1) is composed by a:

- EJ-200 plastic scintillator prototype detector for gamma-rays, with 110 mm in diameter and 30 mm deep with a 32 μm titanium window to improve beta particles detection.

- EJ-426HD plastic scintillator for thermal neutron detection, with two layers of 25×90 mm2 and 0.32 mm deep (6Li is part of its composition). In order to have a neutron detection system also sensitive to fast neutrons (normally emitted by neutron sources) it was necessary to develop a high-density polyethylene (HDPE) moderator. This moderator is rich in hydrogen atoms and is used to reduce the neutron's energy (mainly by elastic collisions with hydrogen nuclei, a process known as thermalization) [6]. Figure 1 shows the EJ-426HD detector embedded in a compact and modular HDPE moderator. HDPE sheets can be introduced or removed depending on the neutron source being detected (neutron energy distribution) and if it is shielded or not (if moderation happens on the cargo material or other shielding material less HDPE moderator sheets are necessary).

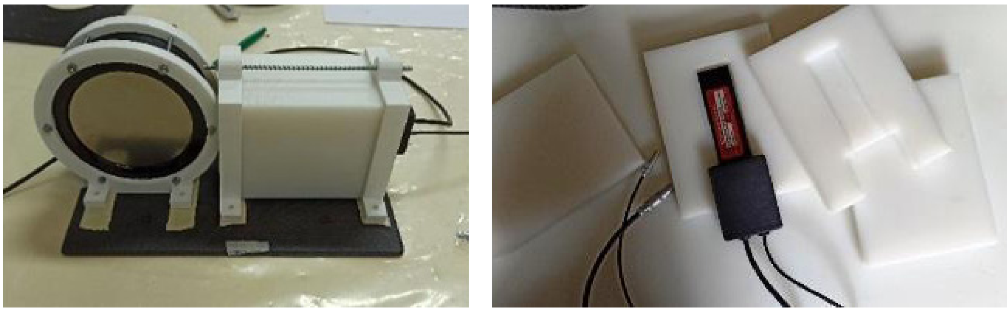


Figure 1. Developed mobile radiation detection system (left image) [5] and detail of the EJ-426HD thermal neutron detection system with HDPE moderator sheets (right image) [6].

The radiation measurements from both detectors are timestamped and georeferenced. In order to have timestamped information from all sensors (detectors and GNSS antenna) it was necessary to perform a clock synchronization of the local computer (Raspberry Pi) with the GNSS clock.

For the radionuclide identification step another payload is being developed, composed by an inorganic scintillator of thallium-doped cesium iodide – CsI(Tl) with 51 mm in diameter and 51 mm in depth with SiPM sensors. The drone payload composed by the plastic scintillators can be easily changed by a second payload composed by the CsI(Tl) detector using the same hardware architecture shown in Figure 2. Another solution could be the use of a fleet of drones (or other mobile platforms) where each platform carries different radiation detection systems with specific purposes (e.g. detection or identification).

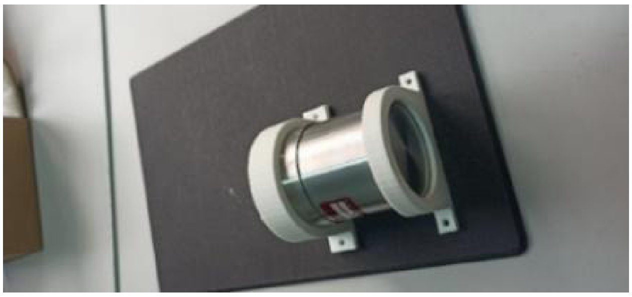


Figure 2. CsI(Tl) scintillator for radionuclide identification (second payload).

The hardware architecture used in this work is shown in Figure 3 and it consists of a power bank, a GNSS antenna, a Topaz-SiPM MCA, and a raspberry pi which can be accessed remotely via Wi-Fi. A laptop and a dedicated router (or a mobile phone hotspot) can be used to access the radiation and GNSS data in real time.

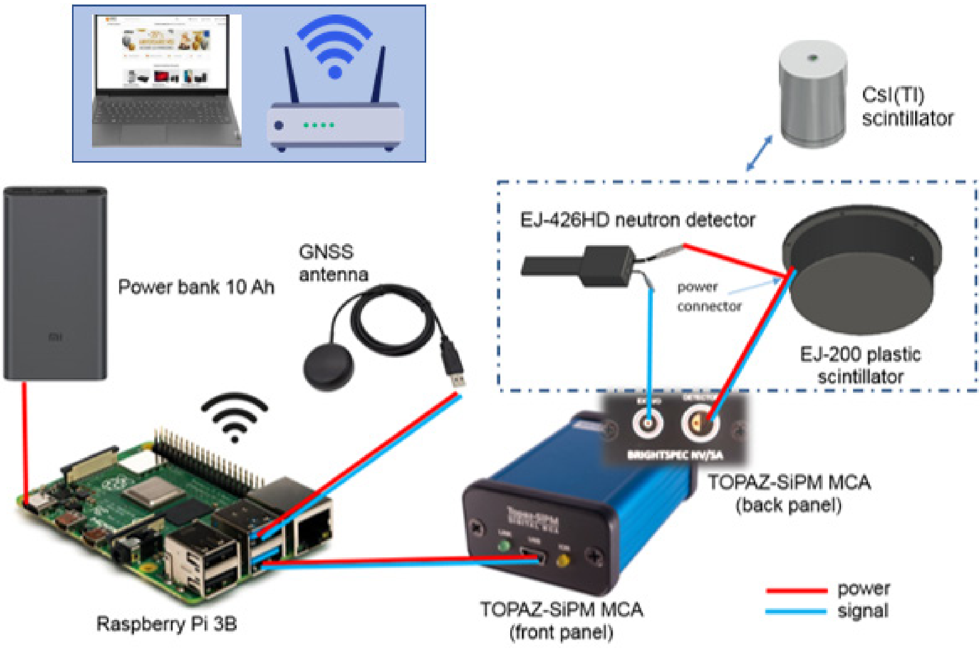


Figure 3. Hardware architecture of the mobile radiation detection system. Adapted from [5].

Currently, the radiation detection system is available either as a handheld equipment and integrated in a multirotor (as shown in Figure 4) and presents a total weight of 2.8 kg (including associated electronics and supports). Since it has an independent power supply and GNSS antenna it can easily be integrated in any other mobile platforms (ground, aerial or hybrid).

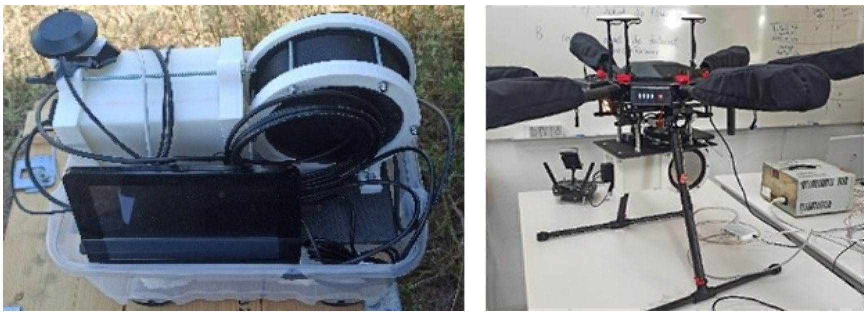


Figure 4. Developed handheld equipment (left image) and radiation detection system integrated in a multirotor DJI Matrice 600 Pro (right image) [5].

2.2. PARTICLE TRANSPORT SIMULATION, LABORATORY AND FIELD TESTS

Radiation particles transport simulation was obtained by using the state-of-the-art program Monte Carlo N-Particle (MCNP) 6. This software simulates the detector geometry and material composition, intermediate medium (normally air) and the radioactive source (point sources). In addition, the software estimates the detection efficiency of different configurations of the plastic scintillators as well as to compare the simulation results of the EJ-200 prototype detector with a commercial CsI(Tl) scintillator. Another simulation result was the optimization of the HDPE moderator geometry and composition to obtain the best EJ-426HD detection efficiency.

Laboratory tests using real gamma, beta, and neutron sources were also performed using the mentioned radiation detection system.

Finally, field tests were carried out using hidden radioactive sources inside a maritime shipping container (standard 20-foot-long container). Using the handheld equipment and the radiation detection system coupled to the drone, lateral and complete turns to the shipping container (three different heights were considered: one third, one half and two thirds the container height) were performed for detection and localization purposes respectively.

3. RESULTS AND DISCUSSION

From MCNP simulation of the EJ-426HD neutron detection system it was obtained an optimal thickness of 7 cm and an area of 14.5×11 cm2 for the moderator sheets in order to maximize the detection efficiency to an Am-Be source. This result was validated by experimental data [6].

EJ-200 showed a factor of 1.59 and 1.49 higher detection efficiency than the commercially available CsI(TI) for source distances of 1-5 m respectively. Since EJ-200 is not a hygroscopic material (unlike most of the inorganic scintillators) it was possible to use a very thin window which allowed to obtain a factor of 1.68 higher beta particle detection efficiency compared to CsI(TI). Laboratory tests allowed to validate the MCNP simulation results [5].

Field tests consisted on the screening of a shipping container with the real gamma and neutron sources using the developed mobile radiation detection system, handheld and drone version (Figure 5), by performing lateral wall and complete turns to the shipping container [5].

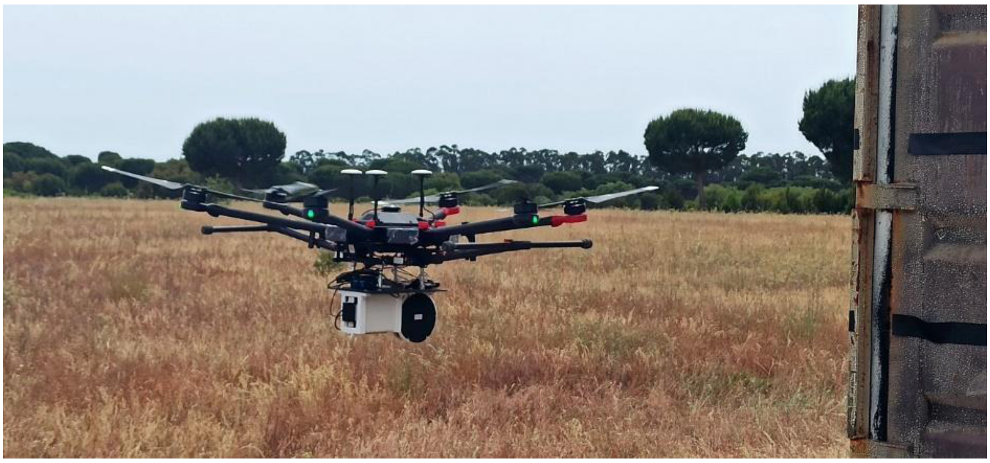


Figure 5. Radiation detection system performing inspection to a shipping container.

Field test results are summarized as follow [5]:

- A 4 MBq 137Cs gamma-ray source placed in the middle of a shipping container was detected during lateral wall inspection (despite it took about 50 s to perform each inspection, this time can be reduced up to 30 s considering only the shipping container length of 6 m). Although this source could be detected, it corresponds approximately to the minimum detectable activity. When the source was placed at the closest corner of the shipping container it was registered a peak on the gamma-ray count rate when the detection system passes near the source´ position.
- When a 1.45 GBq Am-Be neutron source was placed at the center and at the closest corner of the shipping container it was obtained a factor of 4-6 higher count rate than the background level respectively when the detection system performed either lateral and complete turns to the shipping container. A rough source position estimation was also possible (top, middle or bottom of the shipping container) when performing the inspection at three heights.
- For localization of the 4 MBq 137Cs gamma-ray source, complete turns to the shipping container using either the handheld equipment or the radiation detection system coupled to the multirotor were performed (2-3 minutes duration each complete turn). From the detector readings and using a maximum likelihood algorithm

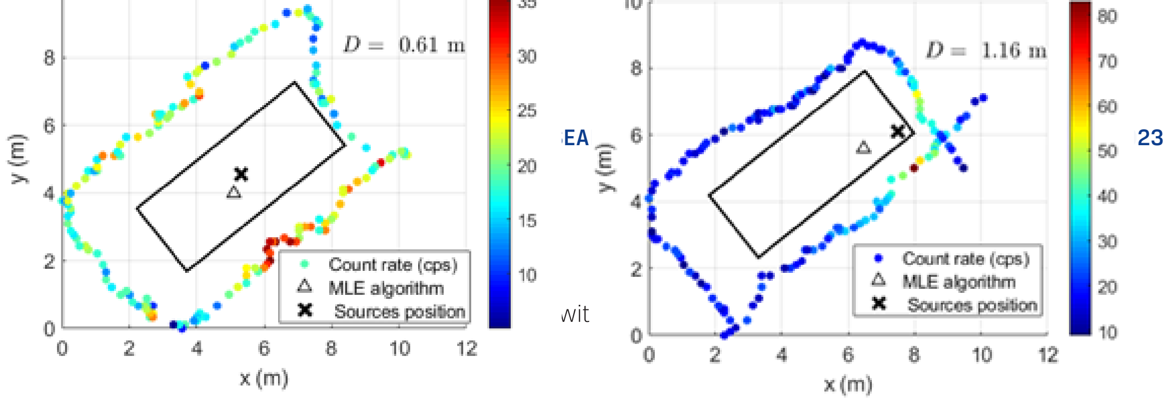


Figure 6. Localization of a 4 MBq 137Cs source placed in the center (left image) and at the corner (right image) of a shipping container using the radiation detection system coupled to the drone [5]. "D" is the distance between the real source position and the estimated position.

Considering that the drone speed was 0.2 m/s and that it has an autonomy for 20 minutes, it would be possible to perform lateral inspection to approximately 44 shipping containers and could reduce the secondary inspection time currently performed by handheld equipment by a factor of 10 avoiding unnecessary radiation exposure risks to the equipment operator. Table 1 resumes the advantages and drawbacks of the mobile radiation detection system.

Table 1. Advantages and disadvantages of the developed mobile radiation detection system.

Radiation detection system characteristic	**Advantages**	**Drawbacks**
Independent power supply and GNSS antenna	Can be easily integrated in any mobile platform or used as a handheld equipment	Not using available antennas and batteries of the mobile platform
Plastic scintillators	Low cost, fast response, variable shape and size, high efficiency to beta particles and neutrons	Cannot perform gamma spectroscopy
EJ-200 scintillator with a very thin titanium window	High sensitivity to beta particles	More fragile window and expensive.
Silicon photomultiplier sensors	Reduced weight, compact, low power consumption, no magnetic field interference	Detector gain must be compensated due to temperature dependence
Neutron detector material based on 6Li	Lightweight, compact and an alternative to 3He based detectors	Lower detection efficiency
Integrated in a multirotor (drone)	High maneuverability, hover and vertical take-off and landing capability	Payload restriction and reduced operation time

This project is characterized by some innovations and disruptiveness in areas such as:

- *Material Science and engineering*. The combination of plastic scintillation materials with SiPM sensors, which gives the best detection efficiency per weight. Also allows their integration in small unmanned vehicles such as drones.
- *Radiation detection methodology*. Based on a two-step process it prioritizes the fast detection, localization and rough quantification of radioactive sources. The radionuclide identification and its exact quantification comes in a second step, e.g. using a second payload with gamma spectroscopy capability or by using a fleet of unmanned vehicles each of it with specialized functions (e.g. detection/localization or identification).
- *Technology application*. Potential for dual use (civil and military), since it is an important tool for homeland security (front line officers), as for the inspection of infrastructures (e.g. shipping containers, nuclear facilities) as well as for Defence applications (military use) when used by Chemical, Biological, Radiological, Nuclear and explosive (CBRNe) response teams. Another growing application is nuclear forensics, where a radiation detection system coupled to a drone can have an important role by avoiding cross contamination.

Moreover, the possible integration of other sensors on the drone such as chemical, biological and explosive sensors, could provide an all-threat approach when dealing with CBRNe defence.

Since active research is ongoing, for example in the search for new plastic scintillator materials and silicon photomultiplier sensors with improved characteristics (less temperature dependence), a long-term use of this technology is also expected.

4. CONCLUSIONS

For nuclear and radiological threats prevention and response normally large and expensive RPMs for the detection and monitorization of gamma-ray and neutron radiation. This paper presents an alternative or complement to RPMs as well as for handheld equipment used to perform secondary inspections to suspected cargo, for example maritime shipping containers. It is also an alternative to other expensive and low detection efficiency mobile radiation detection systems used nowadays in Security and Defence scenarios.

A low cost, low power consumption and high detection efficiency mobile radiation detection system based on plastic scintillators with SiPM sensors was developed. This radiation detection system can simultaneously detect gamma-rays, beta particles and neutrons and can be used as handheld equipment or can be integrated in any mobile platform. Moreover, it is proposed a nuclear and radiological threat approach methodology based on the fast detection and localization of radioactive materials followed by the radionuclide identification and quantification using a second payload (changing the payload) or using a specialized drone with a detection system with spectroscopy capability. The mobile radiation detection system can detect gamma-rays, beta particles and neutrons (thermal and fast component) and to localize gamma-ray sources with a precision of about 1 m using a maximum likelihood algorithm. Besides it can perform primary inspections to shipping containers below 1 minute it also allows to reduce the inspection time by a factor of 10 compared to handheld equipment.

The developed mobile radiation detection system is also a valuable tool for decision support of national authorities and CBRNe defence teams allowing them to establish safe areas and evacuation plans for population in the case of a nuclear and radiological emergency (e.g. radiological release or nuclear disaster).

The easy reproduction of the radiation detection system will allow its implementation in several platforms allowing to reduce survey or inspection times and to perform autonomous inspections and monitoring using unmanned vehicles. By rotating 90° the EJ-200 detector it is also possible to perform ground contamination mapping.

The lithium-6 based neutron detection system is an alternative to the worldwide shortage helium-3 normally used on commercial neutron detectors.

As future work, it will be implemented a second payload with a CsI(Tl) scintillator for identification purposes. This payload can be quicky installed on the drone (removing the payload used to initially detect and localize the radioactive source) or integrated in other drone or mobile platform (e.g. fleet of drones). Finally, it is recommended an all-threat approach by considering the integration of other sensors such as for chemical and biological agents and explosives.

ACKNOWLEDGEMENTS

The authors would like to thank the Portuguese Air Force, in particular Campo de Tiro, Esquadrilha de Defesa CBRN, Kit mobilidade and of Laboratório de Solos e Pavimentos.

REFERENCES

[1] International Atomic Energy Agency. Combating Illicit Trafficking in Nuclear and Other Radioactive Material; IAEA Nuclear Security Series No. 6; International Atomic Energy Agency: Vienna, Austria, 2007; ISBN 978-92-0-109807-8.

[2] International Atomic Energy Agency. Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control: Implementing Guide; IAEA Nuclear Security Series No. 21; International Atomic Energy Agency: Vienna, Austria, 2013; ISBN 978-92-0-142910-0.

[3] E. L. Connolly and P. G. Martin, (2021) "Current and Prospective Radiation Detection Systems, Screening

Infrastructure and Interpretive Algorithms for the Non-Intrusive Screening of Shipping Container Cargo: A Review," Journal of Nuclear Engineering, vol. 2, no. 3, pp. 246–280. doi: 10.3390/jne2030023.

[4] L. Marques, A. Vale, and P. Vaz, (2021) "State-of-the-Art Mobile Radiation Detection Systems for Different Scenarios," Sensors, vol. 21, no. 4, p. 1051. doi: 10.3390/s21041051.

[5] L. Marques et al., (2022) "Neutron and Gamma-Ray Detection System Coupled to a Multirotor for Screening of Shipping Container Cargo," Sensors, vol. 23, no. 1, p. 329. doi: 10.3390/s23010329.

[6] L. Marques, A. Vale, P. Vaz, (2023) "Development of a Portable Neutron Detection System for Security and Defense Applications," in Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies, Á. Rocha, C.H. Fajardo-Toro and J.M. Riola, Eds. Singapore: Springer, vol 328, pp. 283–293. doi: 10.1007/978-981-19-7689-6_24.

Authors

Luís Marques is a Ph.D student in Technological Physics Engineering at the Instituto Superior Técnico (Lisbon, Portugal), is a researcher at Centro de Investigação da Academia da Força Aérea, collaborator researcher at Centro de Ciências e Tecnologias Nucleares and remote pilot of fixed-wing unmanned aircraft system at the Portuguese Air Force.

Pedro Vaz, Ph.D. in Physics, is Coordinator Researcher at Instituto Superior Técnico (IST), the leading Portuguese University of Engineering, Science and Technology, at the University of Lisbon). He is currently member of the Group of Experts (GoE) under Article 31 of the EURATOM Treaty and nominated Portuguese expert at the EURATOM Programme Committee - Fission of the European Union. He is author/co-author of approximately 420 articles published in international journals with peer reviewing and in Conference Proceedings.

Alberto Vale is Assistant Professor at Department of Electrical and Computer Engineering (DEEC) of Instituto Superior Técnico (IST) since 2021 and Senior Researcher at Institute of Plasmas and Nuclear Fusion (IPFN/IST) since 2008. He received the Licenciatura and Ph.D. degrees at IST in 1999 and 2005, respectively. From 1999 to 2005 he was a researcher at the Institute for Systems and Robotics (ISR), working on mobile robotics. From 2006 to 2008 he was Chief RD Engineer and co-founder of Albatroz Engineering S.A. From 2012 to 2017 he was responsible teacher of two classes in the graduation of Othoprosthesis course at Lisbon School of Health Technology of Polytechnic Institute of Lisbon.

A TIERED SERVICE FOR INTEROPERABLE DATA INGESTION AND DISTRIBUTION

Björn Appel, Fulvio Arreghini, Frank Beer, Dennis Füller, Peter Gorski[1]

Abstract

The European Union finds itself again at the center of a geopolitical crisis and must cope with new challenges, such as the weaponization of information. This can be seen with disinformation campaigns, as well as important cyber-attacks on critical infrastructures. This not only involves military and public authorities but also private, non-military entities.

This threat evolution requires EU Member States and Institutions to rethink and adapt their post-conflict reconstruction strategies, by making sure that the data is flowing securely between all necessary actors in a degraded/disabled infrastructure.

The solution described in this paper is based on an innovative tiered architecture, which guarantees secure ingestion and distribution of data (extracted from heterogeneous sources) during a post-conflict phase. The use of AI-based trust and risk models - together with solutions for protecting data domains transitions - is demonstrated to allow for reliable data quality check and data protection.

Keywords

Post conflict management, civil-military cooperation, cybersecurity, command and control systems.

1. THE CYBERSECURITY PERSPECTIVE OF POST CONFLICT RESOLUTION

After decades of relative stability, the European geopolitical scenario has become again the center of a potentially large-scale crisis. European Member States are facing unprecedented challenges requiring them to cooperate efficiently and fast to cope with a rapidly evolving situation. The actors of this complex international situation are not anymore limited to military forces, but involve governmental organizations and even non-military assets like critical infrastructures. A common denominator of the ongoing crisis is the weaponization of information, in various grades of 'intensity' from the disinformation to the extensive use of cyber attacks. It is then clear that the availability of the right information to decision makers becomes more than ever a need. In this paper we analyze the specific case of a post conflict reconstruction scenario, as an exemplary case of civil-military cooperation in a disrupted information environment, and propose a novel solution, supported by AI, to enable an efficient flow of information to effectors (e.g. civil contractors).

Recovery from a military conflict poses exceptional challenges for both the affected host nation and allies. Under these circumstances, one must expect a disruption of civilian critical infrastructures e.g. food distribution, power supply, or at least parts of them. In addition, aftereffects may be still underway in the form of adverse events caused by enemy forces hampering assistance activities. In this context, we promote an in-depth civil-military collaboration by proposing a new conceptual blueprint that conflates both fundamentally different stakeholder domains. Its basic idea relies on a tiered service architecture that complements existing (military) command and control (C2) infrastructures towards a holistic information exchange system while facilitating data ingestion of former unused sources and enabling a regulated transfer of specific task order (STO) to civil performers.

[1] INFODAS GmbH, Cologne, Germany b.appel@infodas.de, f.arreghini@infodas.de, f.beer@infodas.de, d.füller@infodas.de, p.gorski@infodas.de

2. DEVELOPING A HOLISTIC APPROACH FOR MILITARY-CIVIL COOPERATION

2.1 THE COLLECTOR AS A SERVICE TIER

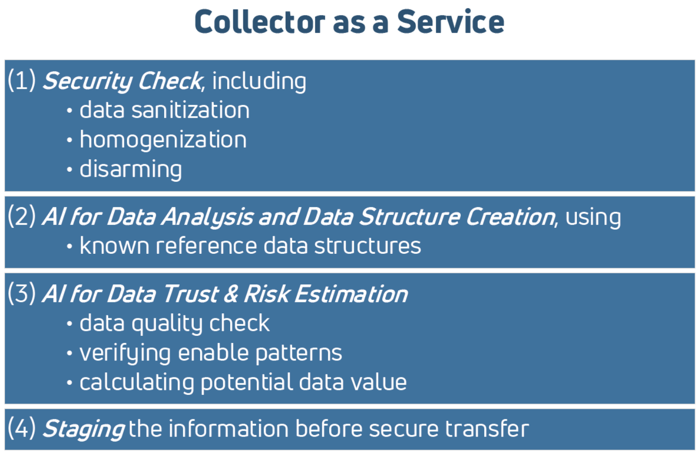
Today, huge amounts of data can be collected from the host nation area to support decision-making by mission commanders. These include classical information sources from allied forces and (European agencies/institutions) or data from open sources like the Internet. Due to the collapse, gathering precise data from the field is a much more difficult endeavor and so highly valuable local information residing in power plants, transport infrastructures or health care facilities remain untouched. Our proposed architecture – see Figure 2- closes this gap and anticipates this challenge through the collector-as-a-service (CaaS) tier. This tier is to integrate data from different data providers (DP) which can be accessed conveniently and securely via public transport networks. To guarantee interoperable and usable integration procedures even in the event of interference where public networks are sabotaged or simply unavailable, our architecture provides DP with further enabler patterns (EP). These give DP actionable instructions suitable for typical use cases considering provided secure and preconfigured reference devices, as well as various available private devices. Thus, building a two-part data foundation sending data to CaaS via mobile (e.g. tactical LTE or TETRA) or satellite networks. Besides the EPs, CaaS implements at least four main big data processing steps (see figure 1) right before ingestion. These include

(1) a thorough security check, data sanitization, homogenization and disarming incoming data before storing.

(2) An algorithm based on artificial intelligence (AI) creates a holistic data model by utilizing already known reference data structures of enabled DP and allocating unknown raw data to these known or even new data patterns.

(3) An AI-based trust and risk model performs a data quality check by verifying data sources' federated identity, potential risk by verifying applied EP, and potential data value.

(4) Data including a risk profile is staged for a secure transfer into classified and existing C2 infrastructure that in turn are shielded via cross-domain solutions (CDS).


Collector as a Service

(1) ***Security Check***, including
- data sanitization
- homogenization
- disarming

(2) ***AI for Data Analysis and Data Structure Creation***, using
- known reference data structures

(3) ***AI for Data Trust & Risk Estimation***
- data quality check
- verifying enable patterns
- calculating potential data value

(4) ***Staging*** the information before secure transfer

Figure 1 Collector as a Service - 4 Steps to data entry

The CaaS complies with performance requirements in terms of data volume, velocity and variety, which are expected to rise rapidly during operation, but are unknown at design time. Therefore, CaaS is designed around distributed principles concerning hardware and software design and a lightweight communication footprint justifying a scalable data ingestion tier.

Information from the CaaS can be used in C2 systems to provide the required information for the commander. After the commander's decision, an STO has to be delivered for example to a civil transport performer. This STO to transport essential equipment (e.g., medical goods, foods, air defense systems, weapons) contains classified, i.e. confidential, information (date, time, origin, destination, route) to fulfill the commander's decision. Typically, the transfer of classified information requires accredited equipment, secured channels, and security-checked personnel. These requirements prevent the delivery of classified STO to civil performers. The introduction of a new security classification for civil performers overcomes these restrictions and enables a regulated transfer of classified information to civil performers.

Current C2 infrastructures are mainly designed to deliver task orders to military performers. With initiatives like the PESCO Project Strategic C2 system for CSDP missions and operations (EUMILCOM), Europe has defined the clear ambition to bring C2 capabilities out of the closed group of military users to enable integrating *all kinds of Communication and Information Systems (CIS), Intelligence Surveillance and Reconnaissance (ISR) and Logistic (LOG) means and will be interoperable with Member States (MS), EU forces, NATO and civil agencies*[2]. Our proposal ensures that the different stakeholders in a complex and multi-tiered C2 infrastructure, can rapidly and seamlessly share critical information protecting their confidentiality, integrity, availability and preserving their trustworthiness, see Figure 2.

2.2 THE DISPATCH AS A SERVICE TIER

A new STO dispatch as a service (DaaS) is responsible for sending STO with the new classification to civil performers. The C2 system and the DaaS connect via a service interface and CDS to prevent classified data leakages. The DaaS adds a verification label to the STO and encrypts the message. The encrypt and decrypt mechanisms as well as the hardware vary from the standard military system, because of protection reasons in case the equipment falls into the hands of opposing forces. The STO reaches the civil performer via the Dispatch Network by using a suitable communication infrastructure (e.g., satellite network, VHF-radio) and approved hardware for communication to establish a secure channel. The civil performer can send status reports via the same secured channel to the mission HQ. This tiered service can be set into place with other governmental or non-governmental organizations as well.

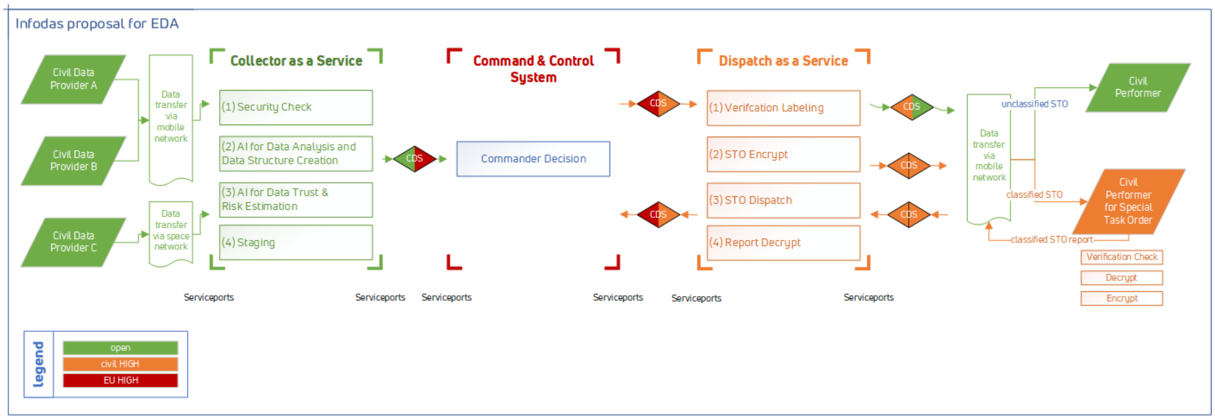


Figure 2 CaaS and DaaS Workflow

References

[1] PESCO.EUROPA.EU, "Strategic C2 System for CDSP Missions and Operations (EUMILCOM)", Strategic C2 System for CSDP Missions and Operations (EUMILCOM) | PESCO (europa.eu), accessed on 31.03.2023

[2] Strategic C2 System for CSDP Missions and Operations (EUMILCOM) | PESCO (europa.eu)

Authors

Dr. Björn Appel, Principal IT Consultant Aviation & Space has a long working experience in the Air & Space sector. In each of his work positions, he participated to the development of new research methods, innovative technologies, and software development capabilities.

Dr Fulvio Arreghini, Head of International Sales is a CDR of the Italian Navy (reserve). He has an Master Degree in communication engineering and a PhD in Information engineering. His research field in the military domain have been mainly secure tactical communications and information security. During his 23 years of active service in the Navy he has been working in the areas of Secure Tactical Communication and Command and Control systems, cybersecurity. He has covered different roles in national and international organizations, including Technical Section leader of the ESSOR Program (EDA Cat B Project later on PESCO/EDF project) at OCCAR and he has been member of different working groups in EDA, NATO and Wireless Innovation Forum. Since 2020 in the private sector, he joined Infodas at first as solution architect to later become head of international sales

Frank Beer, Senior IT Consultant, is specialised in Artificial Intelligence and Explainable Machine Learning. He has a master's in computer science and wrote his master´s thesis at the Fraunhofer Institute FIS.

Dennis Füller leads the IT Security Consulting Defense unit which supports the German Armed Forces and the defense industry. He joined infodas in 2016 after his military service as an officer in the German Armed Forces, where he served in several leadership positions with close relationship to information technology and as an security officer with advisory and audit responsibility for both military services and defense industries. Dennis studied at the University of the German Federal Armed Forces in Munich and at the Ruhr-University Bochum

Dr. Peter Leo Gorski, Lead R&D Science & Innovation, leads a research group at INFODAS GmbH Germany. His research interests include security-enhancing technologies for critical infrastructures and software development processes. Gorski received a Ph.D. in computer science from TU Berlin, Germany.

GNN-BASED DEEP REINFORCEMENT LEARNING WITH ADVERSARIAL TRAINING FOR ROBUST OPTIMIZATION OF MODERN TACTICAL COMMUNICATION SYSTEMS

Johannes F. Loevenich, and Roberto Rigolin F. Lopes[1]

Abstract

This paper investigates the feasibility of a Graph Neural Network (GNN)-based Deep Reinforcement Learning (DRL) for tackling complex optimization problems in modern communication systems deployed to tactical networks. Our methodology consists of three interacting agents: an environment builder agent responsible for generating complex network graph environments, a DRL agent situated within the control plane that possesses a global view of the current network state and makes decisions based on information gathered from various layers of the multi-layer tactical system, and an adversary designed to perturb the DRL agent, thereby evaluating its performance and robustness against data perturbations. Our numerical results indicate that enabling GNNs in conjunction with adversarial training is crucial for the agent to learn the underlying network topology and parameters, ultimately enhancing the robustness of modern tactical communication systems operating in hostile environments.

Keywords

Adversarial Attacks, Reinforcement Learning, Graph Neural Networks, Tactical Communication Systems

1. INTRODUCTION

Recent investigations introduced Machine Learning (ML) models operating across multiple protocol layers to handle ever-changing communication scenarios in tactical networks [1, 2, 3]. Remember that tactical networks are heterogeneous Mobile Adhoc Networks (MANETs) deployed by the military to contested regions, where active adversaries may launch kinetic or cyber attacks on communication systems. Therefore, tactical communication systems must handle ever-changing communication scenarios including cyber attacks from adversaries. The present investigation starts with the hypothesis that Deep Reinforcement Learning (DRL) models within tactical communication systems must undergo training and testing against a broad spectrum of scenarios, encompassing adversarial attacks, to achieve an adequate level of robustness and reliability. The objective is to introduce a training methodology that builds upon and extends previous research aimed at enhancing the robustness of Reinforcement Learning (RL) models by incorporating adversarial attacks [4, 2]. As a result, this approach enables agents to challenge one other until the RL model converges to a parameter set capable of handling ever-changing scenarios, including attacks from an adversary.

The motivation comes from the fact that military personnel goes through a difcult training program before being deployed to hostile environments like battlefelds. Consequently, our three-agent establishes a challenging training and testing regimen for the Graph Neural Network (GNN)-based DRL agent. More precise, we examine a network scenario based on Software Defned Networking (SDN) generated by an environment builder agent. Within this scenario, the DRL agent, located within the control plane, has a global view of the current network state, which may perturbed by the adversary, and must make decisions based on information gathered from various layers of the multi-layer tactical system. In short, the contributions of this paper include the following: (1) defning network scenarios encompassing a multi-layer environment within tactical

[1] Secure Communication & Information (SIX) - Thales Deutschland, Ditzingen, Germany
{johannes.loevenich, roberto.rigolin}@thalesgroup.com

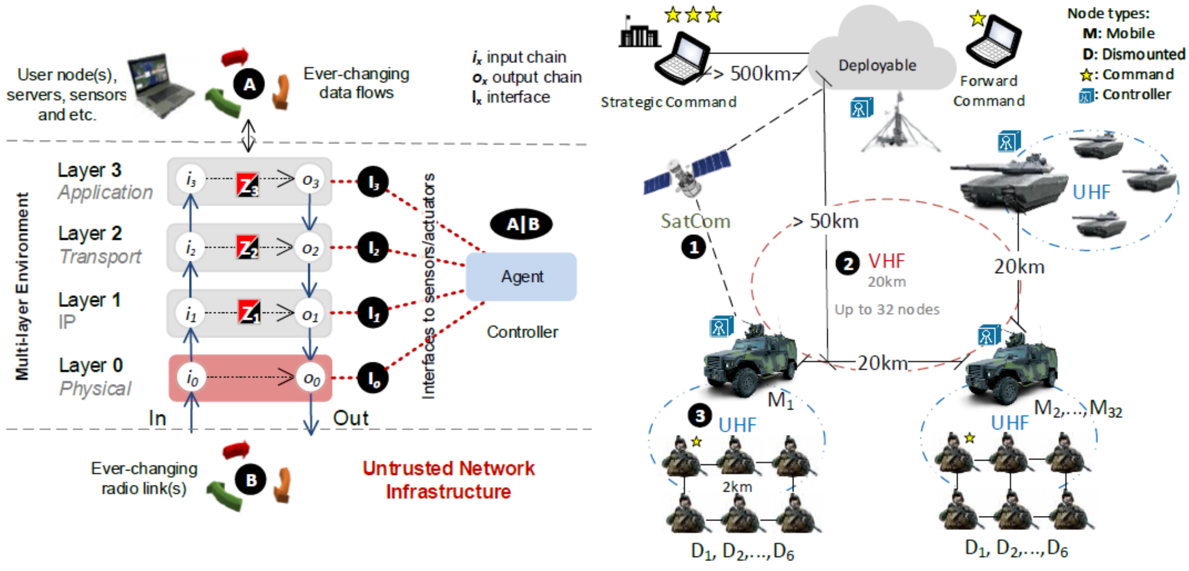
communication systems, where intelligent agents can monitor and actuate (e.g. from a SDN controller); (2) developing a GNN-based RL agent capable of solving complex optimization problems in the environment; and (3) introducing an adversary and a robustness metric to evaluate and enhance the performance of the DRL agent through adversarial training.

The remainder of the paper is structured as follows: Section 2 discusses the core concepts supporting this investigation, namely multi-layer tactical communication systems, GNNs and RL. Section 3 outlines the models for the three agents and details the adversarial training methodology. Section 4 presents numerical results and analysis. Lastly, Section 5 outlines directions for future research.

2. BACKGROUND

2.1. ENVIRONMENT: MULTI-LAYER TACTICAL COMMUNICATION SYSTEMS

The tactical communication system is the environment where intelligent agents can monitor and actuate in diferent protocol layers. These systems are composed of a set of networking devices providing the means for wireless communications at the edge of tactical networks, such as one or more tactical radios, switches, communication servers, controllers and user facing node. The present investigation assumes that modern tactical systems include distributed SDN controllers hosting intelligent agents monitoring/actuating in dif- ferent layers of the system. For example, Figure 1a shows an abstract representation of a multi-layer tactical communication system with four layers, namely physical (0), IP (1), transport (2) and application (3) lay- ers. The incoming and outgoing chains in each layer compose the multi-layer environment where intelligent agents can monitor and actuate. Complementing, Figure 1b shows an exemplary heterogeneous tactical net- work with three types of nodes (deployed, mobile and dismounted) and three communication technologies (SatCom, Very High Frequency (VHF) and Ultra High Frequency (UHF)). These networks are exposed to several random efects (e.g. node mobility, obstacles and adversaries) that will change the link quality and by consequence the network topology.



(a) Multi-layer tactical communication system

(b) Heterogeneous tactical network

Figure 1: Exemplary multi-layer system (a) and heterogeneous topology (b) of tactical networks.

2.2. AGENT: DEEP REINFORCEMENT LEARNING USING GRAPH NEURAL NETWORKS

In this paper, we present a novel approach that integrates two ML techniques. Firstly, we employ a GNN to represent various tactical network scenarios. GNNs are specialized neural network models tailored for handling graph-structured data, providing near-instantaneous performance on the order of milliseconds. Sec- ondly, we utilize

DRL to construct an intelligent agent capable of efectively managing networks in pursuit of a specifc optimization objective. DRL leverages insights from prior optimization experiences for subse- quent decision-making, eliminating the need for executing resource-intensive algorithms.

2.2.1. GRAPH NEURAL NETWORKS

GNNs constitute an innovative class of neural networks specifcally engineered to function with graph-based data. At their core, GNNs involve assigning initial states to distinct elements within an input graph and sub- sequently combining them based on the graph's connectivity. An iterative process updates the elements' states, utilizing the resulting states to generate output. The problem's unique characteristics determine the most suitable GNN variant, contingent on factors such as the graph elements' nature (i.e., nodes and edges). Message Passing Neural Networks (MPNNs) represent a widely recognized subclass of GNNs, which em- ploy an iterative message-passing algorithm for information propagation among graph nodes. During a message-passing step, each node k acquires messages from neighboring nodes, denoted by N(k). These messages are generated through the application of a message function, m(·), to the hidden states of node pairs within the graph. The messages are then integrated via an aggregation function, such as a summation. Lastly, an update function, u(·), computes a new hidden state for every node.

$$\begin{aligned} M_k^{t+1} &= \sum_{i \in N(k)} m(h_k^t, h_i^t) \\ h_k^{t+1} &= u(h_k^t, M_k^{t+1}) \end{aligned}$$

In these equations, functions m(·) and u(·) can be learned through neural networks. After a predetermined number of iterations, the fnal node states are employed by a readout function, r(·), to generate output relevant to the task at hand. This function, often implemented by a neural network, typically predicts individual node properties (e.g., node class) or global graph properties. GNNs have demonstrated signifcant performance in various domains where data is inherently structured as a graph. Given that tactical networks are graph- based, GNNs inherently provide unique advantages for network modeling compared to conventional neural network architectures, such as fully connected Convolutional Neural Networks (CNNs).

2.2.2. DEEP REINFORCEMENT LEARNING

DRL algorithms strive to learn a long-term strategy that maximizes an objective function in an optimization problem. DRL agents commence from a clean slate and iteratively learn the optimal strategy by exploring the state and action spaces, denoted by sets S and A, respectively. Given a state s ∈ S, the agent executes an action a ∈ A, transitioning to a new state **s′** ∈ S and receiving a reward r. The ultimate goal is to discover a strategy that maximizes cumulative reward by the end of an episode, with the episode's conclusion being dependent on the specifc optimization problem. For example, Q-learning is a RL algorithm that teaches an agent to learn a policy π : S → A. The algorithm generates a table, q-table, containing all possible state- action combinations. Initially, the table is populated with zeros or random values, and the agent updates these values during training based on the rewards obtained from chosen actions. These values, known as q-values, represent the expected cumulative reward after applying action a from state s, assuming the agent adheres to the current policy π for the remainder of the episode. Q-values are updated using the Bellman equation (Eq. 2) where Q(st, at) is the q-value function at time-step t, α denotes the learning rate, r(st, at) signifes the reward obtained from selecting action at from state s.t., and γ ∈ [0, 1] is the discount factor.

$$Q(s_t, a_t) = Q(s_t, a_t) + \alpha \left(r(s_t, a_t) + \gamma \max_{a'} Q(s'_t, a') - Q(s_t, a_t) \right)$$

2.3. MOTIVATION: DATA SENSITIVITY AND MILITARY TRAINING

This research is motivated by two key factors: the sensitivity of real-world data in tactical networks and the rigorous training undergone by military personnel. Both aspects infuence the development of intelligent agents and their ability to support human users in high-stakes and ever-changing environments. Obtaining real-world military logs for model training in tactical networks is challenging due to the sensitive nature of the data. To address this issue, RL models can be trained in game-like environments. This approach allows models to learn autonomously, competing against each other without human intervention or data generated by humans. As a result, more robust and adaptive ML models capable of efectively responding to real-world situations can be developed. Furthermore, military personnel undergo intensive training programs to ensure their profciency in using tactical networks. Similarly, intelligent systems and models must be subjected to stringent training regimens, including exposure to extreme communication scenarios. Replicating the chal- lenges faced by military personnel helps develop intelligent agents better equipped to support their human counterparts.

3. DESIGN: THREE AGENTS MODEL

3.1. ENVIRONMENT BUILDER AGENT

The network environment is modeled as a time-dependent, edge-weighted network graph $G := (V, E_t)$, comprising a set of mobile nodes V and radio links E_t at time t. To generate a wide variety of graphs refecting the dynamic nature and requirements that arise from the communication in tactical MANETs and coordination between units in the battlefeld, the environment builder agent AEnv implements a graph model $G(\Omega, n, \nu, S, \delta)$, which accounts for heterogeneous velocity, temporal dependencies, units joining and leaving scenarios, and group movement. To meet these requirements, the model incorporates various confguration parameters, including the size of the mission area Ω, the number of network nodes n, and the velocity intervals for low, medium, and high mobility ν. Additionally, $S \subset N$ represents the link state, which represents the diferent transmission rates of the corresponding network nodes, while δ defnes the minimum link state required for two nodes to be considered connected. During the initialization phase, the mission area Ω can be partitioned into three distinct mobility zones: low, medium, and high mobility. This approach is motivated by the observation that in military scenarios, units in border areas typically move more slowly, while those in the center move more rapidly. To initialize each network node $v \in V$, we randomly sample a starting position $p_v(x, y)$ and assign a velocity $\vec{v} \in \nu_v$ based on its node type (mounted, dismounted) and the mobility zone $\nu_v \in \nu$ to which the node belongs.

After initializing our model G with G0, it evolves with respect to predefned mobility patterns: Random Waypoint, Gauss-Markov, Reference Group Mobility model, or real-world scenarios like Anglova. The network topology is updated by calculating communication areas and edges E_t for each node's movement over time t. As detailed in [5], MANET links exist in one of S link quality states (0 to $S - 1$), with a one- to-one correspondence to the adaptive coding and modulation scheme. To determine link (u, v) state at time t, we partition node u's area into S annular areas, $A_0(u), \ldots, A_{S-1}(u)$, with radii d_{s-1} and d_s, $d_s > d_j$ for $s < j$, $dS = 0$, d_1 as node u's radio transmission range, and $d_0 = \infty$. Link state s occurs when node v is in area $A_s(u)$, with their Euclidean distance in $[d_s, d_{s+1}]$. Once the link state is established, we can use the one-to-one mapping of link states to physical layer (PHY) data rates, to determine the modulation and coding schemes and the subsequent data rate at state s.

To allow for greater variation in the topologies of the network graphs $G_t \in G$, we have implemented the model in such a way that diferent instances can be stacked together to generate scenarios where diferent groups of nodes move according to diferent mobility patterns. By combining multiple instances of the model, we can introduce more heterogeneity in the network, resulting in more complex and diverse scenarios that can help to test the limits of the network's performance.

3.2. GNN-BASED REINFORCEMENT LEARNING AGENT

The network state is characterized by the interrelated topological attributes and features of links and nodes, extracted from various layers within the tactical system. These features are represented by the network graph G_t

at a specifc time t, which is generated by the environment builder agent AEnv. The selection of pertinent features highly depends on the optimization objectives of the agent system under study. For instance, in a routing scenario as elaborated in Section 4., typical features encompass attributes such as link quality (data rate), radio bufer size, and packet loss, as discussed in [2]. Furthermore, link betweenness serves as a feature, which stems from graph theory and quantifes centrality by indicating the number of potential paths traversing a link. This metric proves instrumental in expediting the agent's convergence to an optimal policy.

The design of the action space demands meticulous consideration, as large-scale real-world tactical networks can lead to high-dimensional action spaces. In the context of a routing scenario, for example, taking into ac- count each source-destination pair can render the routing problem increasingly complex for the DRL agent, which must compute estimations for all feasible routing confgurations. Moreover, to ensure the generaliza- tion of the model to previously unseen network topologies, the action space must exhibit invariance to per- mutations of nodes and edges. This implies that a fully trained GNN possesses the capacity to comprehend actions across arbitrary graph structures, encompassing arbitrary network states and topologies. Address- ing this challenge, we restrict the action set to k candidate actions for each node pair within the network. The action representation is integrated into the network's hidden state $h_i = x_1, \ldots, x_D$ via one-hot encod- ing. Consequently, we incorporate additional action-node-link features that exemplify the consequences of executing the corresponding action in the context of the current network state. In a routing scenario, for example, this might involve a link-level feature such as the allocated bandwidth demand for the ongoing trafc request. As a result, the features within the hidden states encapsulate both the network state and the action, providing the essential information for the DRL agent's quality function. An illustrative hidden state representation could be defned as follows: x_1: Link quality, x_2: sender node bufer size, x_3: receiver node packet loss, x_4: link betweenness, x_5: one-hot-encoded action vector, and x_6-x_N : Zero padding. Typically, the size of the hidden states exceeds the number of features present within them. This arrangement allows each link to retain its own initial features in addition to the aggregated information received from all neigh- boring links. If the hidden state size were equal to the number of link features, links would lack the capacity to store information about neighboring links without forfeiting data. Such a scenario would lead to an inad- equate graph embedding following the readout function. In contrast, an excessively large hidden state size may result in a sizable GNN model, potentially causing over-ftting to the data. A prevalent strategy involves setting the hidden state size to be greater than the number of features and populating the remaining vector elements with zeros. This approach mitigates the risk of over-ftting while preserving sufcient capacity for information storage and representation.

Our GNN architecture is inspired by the Message Passing Neural Network in [6]. In our approach, we create an internal graph representation for the GNN by constructing a graph embedding that introduces an ad- ditional node for each link (u, v) situated between sender and receiver nodes. Subsequently, we establish additional links from the sender node to the new link node, and from the link node to the receiver node. Employing this representation, we execute the message-passing process among all nodes. The algorithm uses link and node features of the original network graph as input features x_i and yields a q-value utilized by the DRL agent. The message-passing process is conducted T times, iterating over all nodes within the graph generated using the graph embedding. For each node, its features are combined with those of its neighboring nodes via a fully connected Deep Neural Network (DNN) layer. The outputs of these operations, referred to as messages, are subsequently aggregated using an element-wise sum and then processed through a Re- current Neural Network (RNN). The RNN updates the hidden states with the newly aggregated information. Ultimately, following the message-passing phase, the resulting link states are aggregated once more using an element-wise sum. The outcome is passed through a fully connected DNN, which models the GNN's readout function. The output of this fnal function constitutes the estimated q-value for the input state and action. The RNN is designed to learn the evolution of link states throughout the message-passing phase. As link information propagates across the graph, hidden states accumulate information from increasingly distant links, introducing the concept of time. RNNs, as a Neural Network (NN) architecture, excel at capturing sequential behavior. Furthermore, specifc RNN architectures like Gated Recurrent Units (GRU) address the vanishing gradient problem, commonly encountered in large sequences, by incorporating internal gating mechanisms. This makes RNNs well-suited for learning link state progression during the message-passing phase, even for large T values.

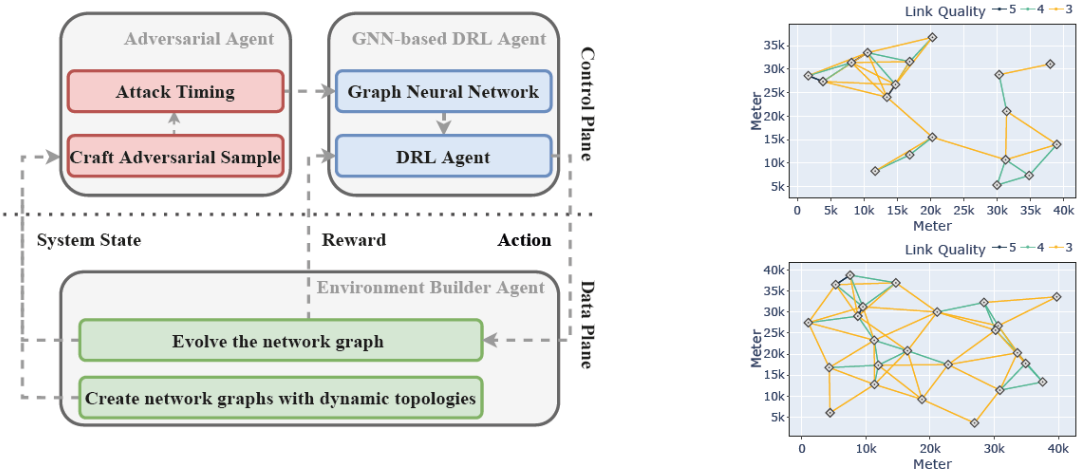
The DRL agent operates by interacting with the environment as described in [2]. Initially, the environment is set up with a network graph generated by the environment agent AEnv, incorporating all link and node features. In a routing scenario, this entails computing the shortest source-destination paths and determining q-values for each of the k candidates using the GNN output. With q-values for each state-action pair, the subsequent action is calculated using an ϵ-greedy exploration strategy. This action is then executed in the environment, yielding a new state s' and a reward r for the DRL agent. Information about the state transition is stored in an experience replay buffer for future GNN training in subsequent episodes.

3.3. ADVERSARIAL AGENT

The adversary $A_{Adv}(s_t) : S \to S$ that perturbs the agent's state observations according to attack timing using crafted adversarial samples (Fig. 2a) is defined by deriving the State Adversarial MDP (SA-MDP) of the underlying Markov Decision Process (MDP) solved by the victim RL agent. Thus, the Markovian Adversary is defined as a deterministic, stationary function that solely depends on the current state at time t. To incorporate realistic constraints, we introduce a perturbation set B(st), which limits the adversary's capability to perturb state st to a pre-established set of states. Consequently, the state adversarial MDP is defined by the 6-tuple (S, A, B, R, p, γ).

The Performance Gap theorem [7] offers a precise upper bound on the difference between value functions when the divergence between two policies is constrained. In essence, the theorem states that the maximum difference in the value functions, under the optimal adversary, is bounded by a constant factor times the maximum total variation distance between the action distributions of the policies under the original state and the perturbed state. The total variation distance is a measure of dissimilarity between two probability distributions, in this case, the action distributions of the policies. Thus, the theorem allows us to quantify the vulnerability of the RL agent to adversarial attacks by providing an upper bound on the performance degradation caused by the adversary. Moreover, the performance gap measure serves as an objective for developing more robust agents using adversarial training. By minimizing this measure, we can train RL agents to be more resilient against adversarial attacks.

As a result, the training methodology involves three interacting agents: the DRL agent A_{RL}, the environment builder agent A_{Env}, and the adversarial agent A_{Adv}, as illustrated in Figure 2a. This figure presents a flowchart depicting the primary steps in the training methodology.



(a) Interacting agent methodology

(b) Gauss Markov model with 18 and 24 nodes

Figure 2: Three-agent methodology (a) and two outputs from the environment builder agent.

4. NUMERICAL RESULTS

4.1. TACTICAL NETWORK ENVIRONMENT

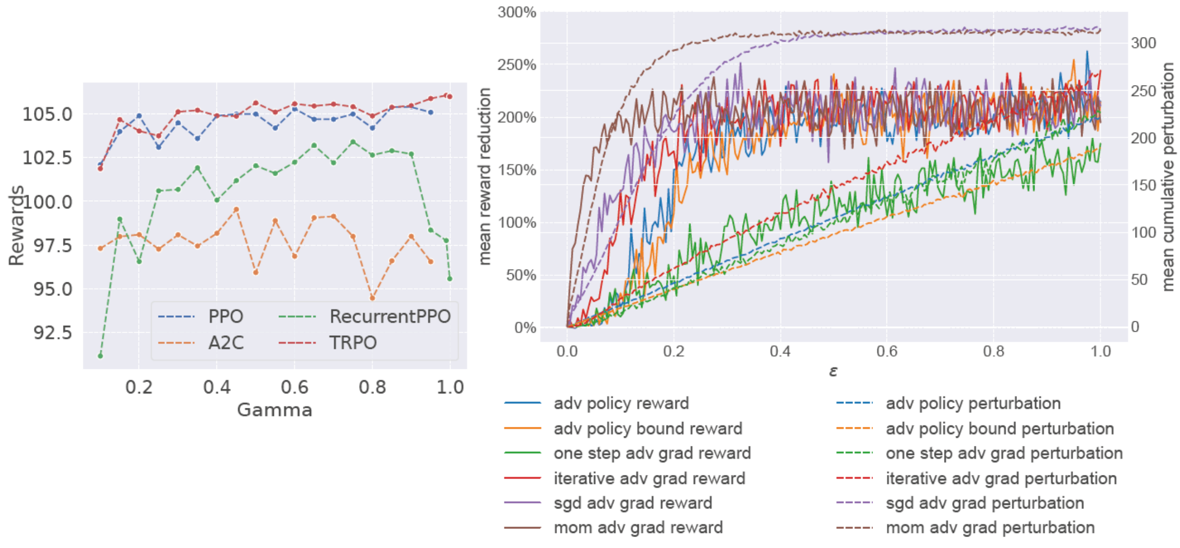
Figure 2b presents exemplary network graphs generated by the environment builder agent A_{Env}, which function as the training and testing environment for the RL agent A_{RL} and adversary agent A_{Adv}. Two graphs created in a mission area Ω = 40km × 40km utilizing Gauss-Markov mobility models with speed intervals ν = [(0.1, 1.5), (4, 10), (10, 25)] in ms–1 (low, medium, high mobility areas), and varying node sizes from 18 to 24 nodes. Diferent link qualities, based on the link model in [5], are indicated by colors ranging from blue (state 5) to red (state 1).

These states are mapped to the radii that bound the respective geographical areas as follows: We compute the histogram (Probability Density Function (PDF)) of pairwise distances between the mobile nodes and map the four radii $d_1, \ldots, d_5$ to percentiles of this distribution. Thus, d_5 corresponds to the 10th percentile, d_4 to the 25th percentile, d_3 to the 45th percentile, d_2 to the 60th percentile, and d_1 to the 75th percentile. This implies that 25% of node pairs are beyond each other's radio coverage. This mapping strategy is employed due to its systematic and controlled approach in the absence of real feld measurements or precise radio propagation and PHY models in emulators like CORE/EMANE.

4.2. DRL AGENT PERFORMANCE EVALUATION

Figure 3a presents a reward comparison for the four top-performing algorithms applied to our DRL agent ARL, which addresses the routing optimization problem outlined in [2] without utilizing the GNN com- ponent. Each data point signifes the mean reward achieved by the corresponding algorithm after hyper- parameter tuning. Our observations indicate that sharing parameters between policy and value function estimators, as implemented in the Asynchronous Advantage Actor Critic (A2C) algorithm, enhances aver- age rewards and maintains relatively consistent rewards above 90 (depicted by the orange line in Figure 3a). However, policy optimization algorithms such as Recurrent Proximal Policy Optimization (RecurrentPPO, shown in green), Trust Region Policy Optimization (Trust Region Policy Optimization (TRPO), shown in red), and Proximal Policy Optimization (Proximal Policy Optimization (PPO), shown in blue) consistently surpass A2C. These fndings imply that the optimization control problem can beneft from constraining the refned policy to remain close to the initial policy, as measured by the Kullback-Leibler (KL) divergence of their respective distributions, either by imposing a stringent trust region constraint as in TRPO, or by employing frst-order optimization on a clipped objective, as demonstrated in PPO.

Upon conducting a more in-depth analysis of the RL agent's internal parameters on large network graphs, it was revealed that the agent failed to learn the underlying graph topology even when achieving high rewards. This issue is commonly encountered when applying RL models to graph theory problems and highlights the necessity for incorporating GNNs to address this challenge. Consequently, this inspired the integration of the GNN component and the associated MPNNs. These networks facilitate information propagation among nodes, allowing for the prediction of individual node attributes (e.g., node class) and global graph properties.



(a) Rewards as a function of gamma

(b) Advanced attack results estimated over 50 episodes with varying ϵ

Figure 3: Numerical results.

4.3. ADVERSARIAL ANALYSIS

Figure 3b presents a comprehensive analysis that compares the performance of various tested attack strategies, including *one-step, iterative*, and *adversarial boosting* attacks. As expected, *one-step* attacks generally exhibit suboptimal performance, with a mean reward reduction that increases linearly with ϵ and reaches a maximum of approximately 150% at $\epsilon = 1.0$. For $\epsilon < 0.3$, *iterative* (or *gradient-based*) attacks slightly outperform adversarial policy attacks; both attack types achieve a maximum reward reduction of 200% at this point. Although the maximum potential of Stochastic Gradient Descent (SGD) is attained at $\epsilon = 0.2$, *momentum-boosted* attacks capitalize on their velocity vector and achieve a reward reduction of 200% more rapidly, at approximately $\epsilon = 0.1$. In general, the experiment indicates that, apart from *one-step attacks*, all attack methods possess the capacity to substantially diminish the victim model's performance by an average of up to 200%.

Combining these fndings with the performance gap theorem proposed in [7], we can conclude that the missing limit on the value functions of the original MDP and the SA-MDP arises from the lack of a constraint on the divergence between $\pi(\cdot|s)$ and $\pi(\cdot|s')$. This highlights the importance of adversarial training in maintaining the divergence between policies within specifc bounds and ensuring the RL agent's robustness against a wide range of data perturbations.

5. FUTURE WORK

In our future work, we aim to address two key aspects to advance our three-agent model. Firstly, we will focus on testing and optimizing the GNN component of the model to enhance information propagation of individual node attributes and global graph properties among nodes, contributing to the development of efcient and robust solutions for complex optimization problems in tactical MANETs. Secondly, we will develop an adversarial training framework that utilizes the adversary agent described in the paper. We have inferred that the absence of a limit on the value functions for the original MDP and the SA-MDP arises from the lack of a constraint on the divergence between both policies. Consequently, the adversarial training framework will maintain the divergence between policies within specifc bounds, ensuring the RL agent's robustness against a wide array of data perturbations from attacks.

References

[1] J. F. Loevenich, A. Sergeev, P. H. L. Rettore, and R. R. F. Lopes, "An intelligent model to quantify the robustness of tactical systems to unplanned link disconnections," in 18th International Conference on the Design of Reliable Communication Networks (DRCN), 2022, pp. 1–8.

[2] J. F. Loevenich, J. Bode, T. Hürten, L. Liberto, F. Spelter, P. H. L. Rettore, and R. R. F. Lopes, "Adver- sarial attacks against reinforcement learning based tactical networks: A case study," in IEEE Military Communications Conference (MILCOM), 2022, pp. 986–992.

[3] J. F. Loevenich, P. H. Rettore, R. R. F. Lopes, and A. Sergeev, "A bayesian inference model for dynamic neighbor discovery in tactical networks," Procedia Computer Science, vol. 205, pp. 28–38, 2022, 2022 International Conference on Military Communication and Information Systems (ICMCIS).

[4] Y. Li, W. Jin, H. Xu, and J. Tang, "Deeprobust: A pytorch library for adversarial attacks and defenses," arXiv, 2020.

[5] P. H. L. Rettore, J. F. Loevenich, and R. R. F. Lopes, "TNT: A tactical network test platform to evaluate military systems over ever-changing scenarios," IEEE Access, vol. 10, pp. 100 939–100 954, 2022.

[6] J. Gilmer, S. S. Schoenholz, P. F. Riley, O. Vinyals, and G. E. Dahl, "Neural message passing for quantum chemistry," in Proceedings of the 34th International Conference on Machine Learning, vol. 70, 06–11 Aug 2017, pp. 1263–1272.

[7] J. Achiam, D. Held, A. Tamar, and P. Abbeel, "Constrained policy optimization," in Proceedings of the 34th International Conference on Machine Learning - Volume 70, ser. ICML'17, 2017, p. 22–31.

Authors

Johannes Loevenich is working as a scientist in the Secure Communications & Information Systems (SIX) team at Thales Deutschland in Ditzingen, Germany. He received a BSc. Computer Science and another BSc. in Mathematics from Rheinische Friedrich-Wilhelms-Universität Bonn. Currently, he is pursuing a PhD in Computer Science/Mathematics in the Distributed Systems Department at the University of Osnabrück. He worked as a scientist in the Communication Systems Department (KOM) at Fraunhofer FKIE in Bonn, Germany. His re- search interests include Computer Systems, Computer Networks, Distributed Systems, Data Science, Optimization Theory, Artifcial Intelligence, and Game Theory.

Roberto Rigolin F. Lopes is a scientist at Thales Deutschland in Ditzingen, Germany. Working with the Secure Communications & Information Systems (SIX) team, he has been attacking problems in Computer Networks and Dis- tributed Systems with a particular interest in the performance bounds of tactical systems over ever-changing communication scenarios. His education includes B.Sc., M.Sc., and Ph.D. degrees in Computer Science from three universities in Brazil (UFMT, UFSCar, and USP). During his Ph.D., he also visited an uni- versity in the Netherlands (UTwente) and another in Canada (UOttawa). After his Ph.D., he got a postdoctoral scholarship from the European Research Consortium for Informatics and Mathematics (ERCIM) to join an university in Norway (NTNU). His academic life triggered interesting life experiences, but he has been rebuilding his own education following curiosity freely by reading books on Physics, Mathematics, and Philosophy.

Acknowledgment

The authors would like to thank Bundeswehr for funding the national and international projects developing the background supporting to the present paper. Particularly, BAAINBw (Federal Ofce of Bundeswehr Equipment, Information Technology and In-Service Support) and WTD 81 (Bundeswehr Technical Center for Information Technology and Electronics). Parts of the present investigation were published/discussed in three scientifc conferences, namely DRCN 2021 [1], ICMCIS 2022 [3], and MILCOM 2022 [2].

ADDITIVE MANUFACTURING APPLICATION FOR RESILIENCE IN DEFENCE SUPPLY CHAINS: POOLED CAPACITY HEDGING AS AN HYBRID INSTRUMENT

Andreas Glas[1] and Michael Essig[2]

Abstract

A recent impulse for strengthening defence supply chains is provided by the Russian attack on Ukraine. Defence supply chains face the risk of getting disrupted. At its core, this paper addresses the question how defence supply chains can become more resilient. Additive Manufacturing (AM) is presented as an enabling technology to increase resilience. Although there is always room for technical improvement, this research focuses on an intelligent application of AM in digital supply chains. Therefore, the argument is that the typical process and application idea of decentralized AM capacities for single parts production is suboptimal. In contrast, this research proposes a hybrid approach where AM is most efficient when (1) construction space of AM is fully utilized and (2) AM is in a hedged interplay with traditional supply sources. This approach (pooled capacity hedging) can enhance future defence supply chain capabilities and the availability of supply through digital integration.

Keywords

Additive Manufacturing, Supply Hedging, Sourcing, Supply Chain.

1. INTRODUCTION: ADDITIVE MANUFACTURING AS TECHNOLOGY ENABLER

Additive Manufacturing (AM) is an umbrella term for several manufacturing procedures [1], often also referred to as "3D-Printing". AM encompasses several techniques including binder jetting, directed energy deposition, material extrusion (e.g., fused deposition modeling, FDM), material jetting, powder bed fusion, sheet lamination, and vat polymerization (e.g., stereolithography) [2]. The first AM-process (stereolithography) was invented by Chuck Hull in 1983 [3]. Therefore, AM exists for over 40 years now and has reached a level of technical maturity. All AM-processes share the commonality that, based on a digital representation of the object to be manufactured (CAD data), material is positioned and joined layer by layer until the physical object is created [4]. Generally, AM has the following main technical characteristics:

AM, unlike traditional manufacturing, does not require any tools. Therefore, a wide variety of parts (designs) can be produced one after the other or even synchronously in just one printing process without a great deal of set-up effort.

AM is a compact machine in terms of structure and requires standardized primary materials (raw materials and energy). This facilitates local, decentralized or relocatable (mobile) production.

AM can produce complex and customer-specific component geometries through layered production, which could not be produced at all or only at very high and sharply increasing costs using traditional processes.

AM can be produced at comparatively low investment costs, so that in comparison with traditional delivery routes and in certain constellations (quantity, urgency, relevance) it is definitely economical.

[1] Research Group Defence Acquisition and Supply Management, Bundeswehr University Munich, Neubiberg, Germany andreas.glas@unibw.de

[2] Working Field Procurement, Chair for Procurement and Supply Management, Bundeswehr University Munich, Neubiberg, Germany michael.essig@unibw.de

AM requires a digital drawing file. Modifications to a part can be made, for example, by adjusting the virtual drawing file, allowing improvements to be translated into new parts faster than traditional methods.

Considering these characteristics, it is not astonishing that AM is used in many supply chains, not only in the defence ones [5]. However, reports mostly focus on performance of single parts (e.g. ship propeller in [5]) or report on AM produced tooling. Reports and research get fewer, if AM shall be integrated into the general defence supply chain. Of course, there is also in defence a "slow revolution" ongoing, what means that more and more parts can be or are produced by AM similar to aerospace supply chains [6]. From a purely technical viewpoint, there is the ability to produce almost all parts with additive manufacturing technologies. As a result, this paper concentrates mainly on the *useful application* of AM for defence supply chains. Instead of giving simple "black or white" answers, we refer to existing research and develop a kind of hybrid approach for an integrated AM-backed resilient defence supply chain approach. This refers to three main aspects of existing research results:

1. AM is not a full replacement of traditional manufacturing technologies :"This means that the market for AM is still growing significantly, but it will never replace everything that´s being manufactured." [6]. This statement guides this work to a first research question: How defence supply chains can make use of a meaningful interplay between AM and traditional manufacturing?
2. Another important aspect is that recent research on AM and supply chain management highlights the potential for in-house decentralization instead of procuring the required parts [7]. This is per se surprising, as typically armed forces do not produce parts on their own, but buy them from companies on markets. A specific research view on this is that AM not only allows decentralization, but "that Additive Manufacturing provides good improvements in supply chain performances offering significant benefits in the decentralized solution" [7]. This positive view on decentralization is more or less adopted when analysing defence supply chains. It is acknowledged that "the capacity utilization in a decentralized model is significantly lower but from the military perspective, it [a decentralized model] adds resilience to the capability" [8]. As such, a research focus was on the analysis of decentralized AM capacity utilization that directly supplies military repair centers (workshops) on a tactical level [e.g. 9].
3. AM and stocks are interrelated: On a tactical level the availability of parts in uncertain demand situations (e.g. crisis/war) depends on available stocks. As such, recent research executed at the level of a mechanical battalion stated that the "current AM speed is not able to increase resilience at the depot level, so at present, increasing the spare parts inventory is a better way to improve resilience"[10]. Of course, every production takes longer time to satisfy demand than available stocks at the point of consumption can do. But capital commitment to stocks is limited even in times of crisis. It seems as if research on the design of defence supply chains integrating AM reached a dead end. Decentralization is the key element, but it is alone not sufficient to safeguard efficient and effective AM use. These two points refer to the second guiding research question of this work: How AM capacity can be meaningfully integrated into a defence supply chain.

To answer the outlined questions, this research provides insights into analysis results that built on mixed methods research of the acknowledged research project. This includes case analysis within the German Bundeswehr but also simulation experiment findings. The following sections will explain how an interplay between AM and traditional manufacturing can be organized and how AM capacities could be used to ensure efficiency and effectiveness. This approach combines bundling of demand, digitally pooled capacities and manufacturing hedging. All these terms are explained in detail in the following sections.

The reminder of this research is as follows. The next section strives the requirements for EU defence supply chains. Then, the problem is framed with a phase model of a supply disruption. Next, AM and TM characteristics are matched with these phases. This allows the formulation of a AM hedging supply strategy. This is followed by some considerations about capacity utilization, what provides the basis for formulating a strategy for AM usage (pooled capacity hedging). A conclusion summarized the main findings and provides an overview on the proposed concept.

2. REQUIREMENTS FOR EU DEFENCE SUPPLY CHAIN

The requirements are defined on basis of the Bundeswehr-case. The Bundeswehr requires the best possible material equipment and the timely availability of the demanded products and services are prerequisites for the successful fulfilment of the mission [11]. The equipment of the Bundeswehr should meet the following core features: **Task-oriented:** The equipment corresponds to the full needs of the military units (from systems to spares, repairables, or operating resources). **Structurally appropriate:** The equipment must cover the need for both training, exercise, and operation. **Timely and needs-based provision of operational equipment:** The departments involved shall see themselves as service providers in order to meet the needs of military units in the best possible and timely way. **Demands on the management:** Dynamics, complexity, goal heterogeneity and competition of goals are recognised, therefore it is a requirement of the Bundeswehr to establish a modern management of the equipment and supply, which integrates these framework factors into its planning.

Strategic management approaches have recognized that only a differentiated view of services and products makes sense ("One size does not fit all") [e.g. 12]. In a very similar way, business administration has also developed a differentiation logic for products for procurement and logistics [13]. Supply strategies are differentiated based on demand predictability. Demands that can be easily predicted are to be supplied by efficiency-oriented supply chains, while less predictable demands are to be supplied by agile supply chains. In industrial logic, you can choose the right supply chain - depending on how accurate you can make the forecast. As a result, the supply risks for each product are optimally addressed.

The Bundeswehr is also acting with limited resources and also wants to solve its supply risks in an "optimal" manner. If one follows the business management knowledge, then a differentiation of the demands would be recommended. In fact, this is already done by the Bundeswehr: "The requirements are very diverse and dynamic and must be planned, prioritized and implemented in different ways accordingly. A purchase "off-the-shelve" has to be differentiated from in-house developments."[11]. Essentially, the demand uncertainty is broken down into "good" and "bad" market-availability.

But market availability again depends on the demand situation and its dynamics. Demands (parts) that are actually "well" available in the supposed "normal state" can quickly turn out to be extremely rare (critical parts) if the situation changes. If in a specific situation, namely "peace", demands are supplied via lean supply chains, then bottlenecks and availability problems arise when the situation changes (e.g. to "crisis"). If, on the other hand, demands are supplied by using agile supply chains in order to be prepared for the worst-case scenario, this leads to exorbitantly high expenses for reserves (stocks, flexibility potential). This is the general equipment and supply dilemma of Armed Forces.

3. SUPPLY DISRUPTION

The dynamics of a demand situation are already mentioned. This section will further model the situation of a supply disruption. This can be tied to established research streams on "resilience management" in Business Administration. If one understands the change in conflicts and wars as deviations / disturbances from one's own original expectations and planning, then an interesting intersection arises here for defence supply chain management research.

The typical process of a supply chain disruption can be described as in Figure 1 [14, 15]. A stable situation exists ex ante of a disruption event. After a triggering event an organization can withstand minor disruptions, so that a drop in performance usually only becomes noticeable after a certain trigger severity and a time lag. The depth of the performance decrease and the duration of the performance decrease depends on how the disruption is managed. The basic goal is to achieve a new, stable level of performance. In the best-case scenario, one could come out of a crisis stronger than before.

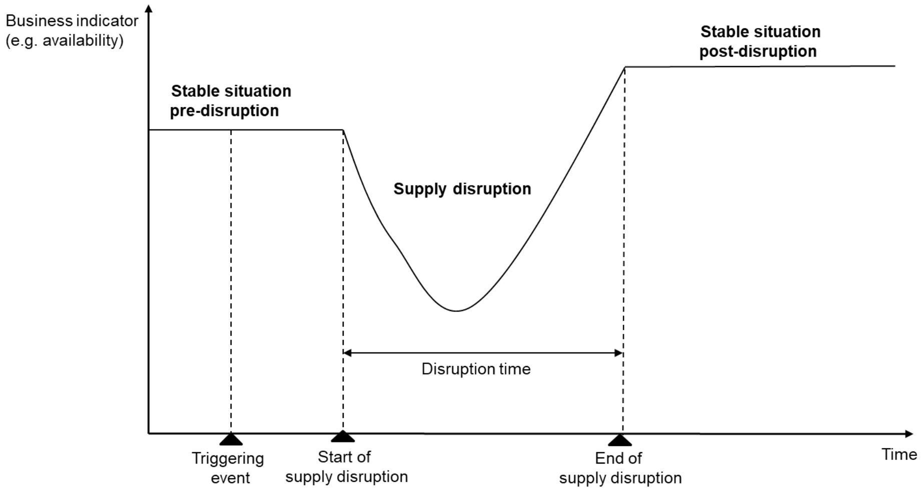


Figure 1. Phases of a supply disruption [14, 15]

Business research distinguishes two major resilience strategies. On the one hand, "robustness". This describes the ability to withstand disturbances. On the other hand, "agility", i.e. the ability to react and adapt to disruptions. One might think that robustness is created ex ante disruption and agility is carried out ex post. In principle, this is true - robustness results, for example, from reserves, stocks, capacities, etc., which of course have to be available before a disruption occurs. Also, agility can only become effective after the disruption, only then is a reaction - e.g. changed prioritization, resource development, etc. - possible. However, the basics of agility (processes, procedures, structures, etc.) are already created ex ante disruption. This is particularly relevant when considering the resilience of armed forces with their phase transitions mentioned above. Overall, this raises the question of the skills and technological instruments that are needed for "strategic agility".

4. THE DIFFERENCES OF AM TO TRADITIONAL MANUFACTURING FROM AN ECONOMIC AND RESILIENCE PERSPECTIVE

AM differs significantly from traditional manufacturing (TM), such as subtractive and formative manufacturing. AM's synonym, direct digital manufacturing [16], incisively describes AM's merits in the transition from the virtual to the physical world. Products can be modified easily by changing the CAD file alone, so one can "press a button" to create the physical product with a 3D printer [1]. This could be used to increase responsiveness in a supply system, as adaption and lead times to respond are reduced.

AM has significantly different cost structures than TM; for example, an increase in a product's geometrical complexity does not lead to additional costs, which makes it indifferent to which type of product to produce [17]. However, the use of economies of scale is highly limited, so AM is mostly used in producing small quantities [18]. Overall, studies found a general time-cost-effect for AM [19], which is illustrated in Figure 2. Typically, AM is faster in production and due to decentralized production sites or smaller packaging sizes even more agile and faster in logistics. But AM is also often costlier in production, as traditional production of a high number of parts has higher economies of scale. Thus, traditional manufacturing plus its logistics is typically slower, but less costly. Coming back to the first guiding question, these characteristics cause the need to orchestrate an interplay between AM and traditional manufacturing.

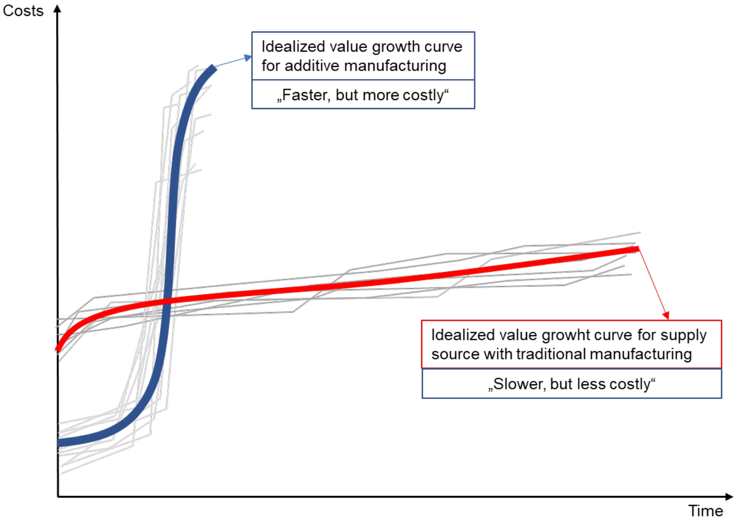


Figure 2. Contrasting time-cost-characteristics of AM and traditional manufacturing

5. HEDGING OF AM

A solution could come from a completely different research stream: financial portfolio and risk management [e.g. 20]. There, they found that it is possible to mix different risk positions in a way that the joint risk exposition is better than only relying to a single alternative. The establishment of a joint risk position that improves the current risk position of single (investment) decisions is called "hedging" [21] A "hedge" describes an (investment) alternative that best offsets potential losses or gains of another (investment) alternative.

The transfer of hedging to supply chain management is not per se new [e.g. 22 for geographical hedging]. But the curves in figure 2 imply that AM and traditional manufacturing also have opposite risk expositions. As such, the idea of hedging might also be applied to manufacturing alternatives in defence supply chains. Figure 3 shows that AM is of course very agile in case of supply disruptions (easy change in production plans, quick change of production site is possible etc.). Therefore, effectiveness risk is low, but efficiency risk is high. The opposite is true for traditional manufacturing. As such, a combination of AM and TM has the potential to optimise the total supply risk ("hybrid solution"). Overall, this does also open the conceptual door for solving research question one. The interplay is not about AM or traditional manufacturing, it is about a parallel usage of both manufacturing sources depending on supply chain vulnerability or supply chain stress.

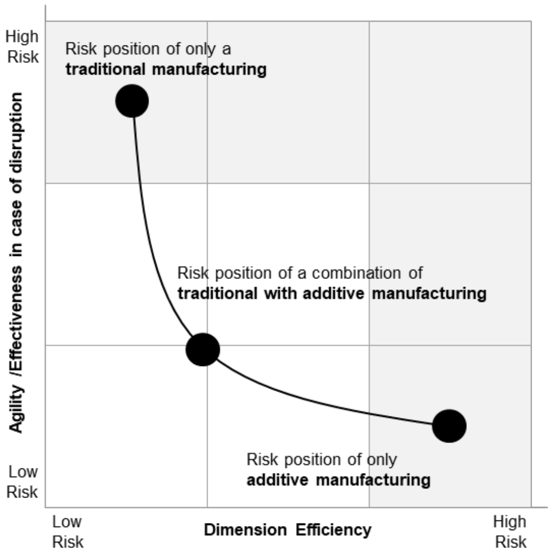

High Risk
Low Risk
Agility /Effectiveness in case of disruption
Risk position of only a traditional manufacturing
Risk position of a combination of traditional with additive manufacturing
Risk position of only additive manufacturing
Low Risk
Dimension Efficiency
High Risk

Figure 3. Combination (Hedging) of AM with traditional manufacturing [19]

6. BUNDLING OF DEMAND AND POOLED USE OF AM CAPACITY

AM possibilities have grown continuously. It is now possible to produce a wide range of individual components using various materials (aluminium, plastic, plaster, steel, composite materials, etc.). It is increasingly possible to use AM (bionic geometries, functional assemblies) that previously could not be manufactured at all. The extrapolation of this manufacturing spectrum shows that in the future, a large part of the parts Armed Forces require will be available using both traditional and AM.

Looking on the costs of a single part form a military user /procurement perspective, AM is currently costlier than in traditional manufacturing as already mentioned above. However, Armed Forces often require small quantities of material. Then, even the cheaper traditional manufacturing does not permanently produce parts but mix production slots with stocks based on forecasts. In other words, orders, production slots, and logistics peaks are managed. Planning could be too optimistic, what causes out-of-stock situations and shortfall costs. Or planning is too pessimistic, what increases capital commitment to stocks (Figure 4 left side). It is the great advantage of AM that it can satisfy demands with batch size one. AM can produce exactly the required quantity, which counteracts storage and logistics costs but also reduces planning uncertainty risks. However, the unit costs are then comparatively expensive because, among other things, the investment costs for the AM capacity are then fully allocated to the single part (Figure 4 middle). But if you print a larger quantity of the same single part, which has a positive effect on the unit costs, you have order peaks and storage costs again, which you actually want to avoid. A focus on single parts is therefore not sufficient to conceptually clarify how AM capacity can be integrated into a defence supply chain.

However, if a sum of potentially demanded parts is taken into perspective (hereinafter referred to as the part portfolio), then AM becomes more efficient. The key is that different parts (product geometries) can be manufactured synchronously in the construction space of a 3D printer. AM requires no tooling, therefore demands of separate demand organizations can be satisfied via the same 3D-printer and thereby allows the pooling of capacities of organizations as shown by [23]. As demands can be manufactured by any potential 3D-printer, more supply sources get available, which can be assigned and utilized in the short term [15]. Of course, the part portfolio must jointly refer to technical specifications (usability of the same printing process, the same raw material and the same type of printer). But then, a high utilization of the AM capacity reduces unit costs of the single part (Figure 4 right side). The portfolio perspective contributes to answer the second research question, because AM can be integrated into defence supply chains, if a sufficient number of demanded parts is identified to ensure full usage of created AM capacities.

By answering this question, this research identified two prerequisites: First, it is necessary to bundle demands. Second, it is required to task AM capacities with print jobs for these bundles of demand parts and to link these capacities with logistics to distribute parts to the recipients. This is possible, as AM only requires CAD-data and thereby stands for a "digital warehouse" on which physical goods can be retrieved "on demand" [24]. As such, one solution for AM management is a digitally enabled, centralized management of (decentralized) AM capacities. This integrates AM into the Defence Supply Chain and supports availability and resilience of supply.

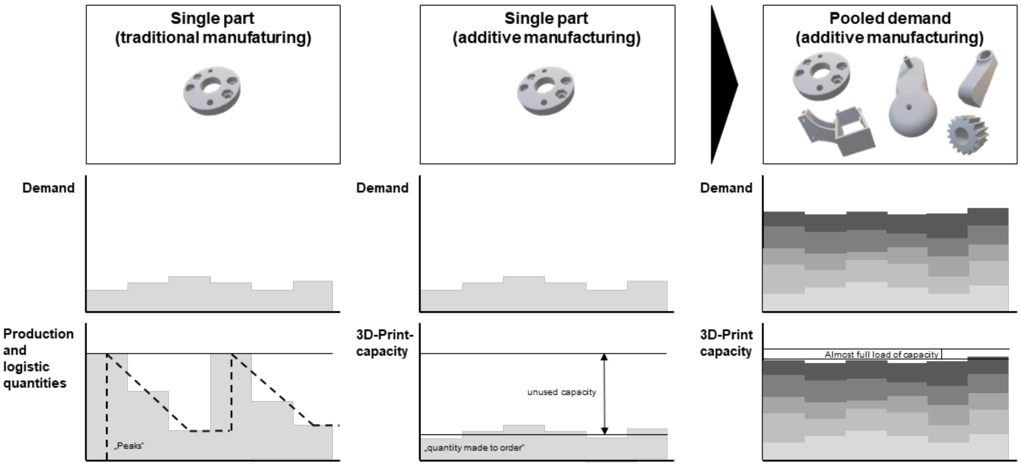


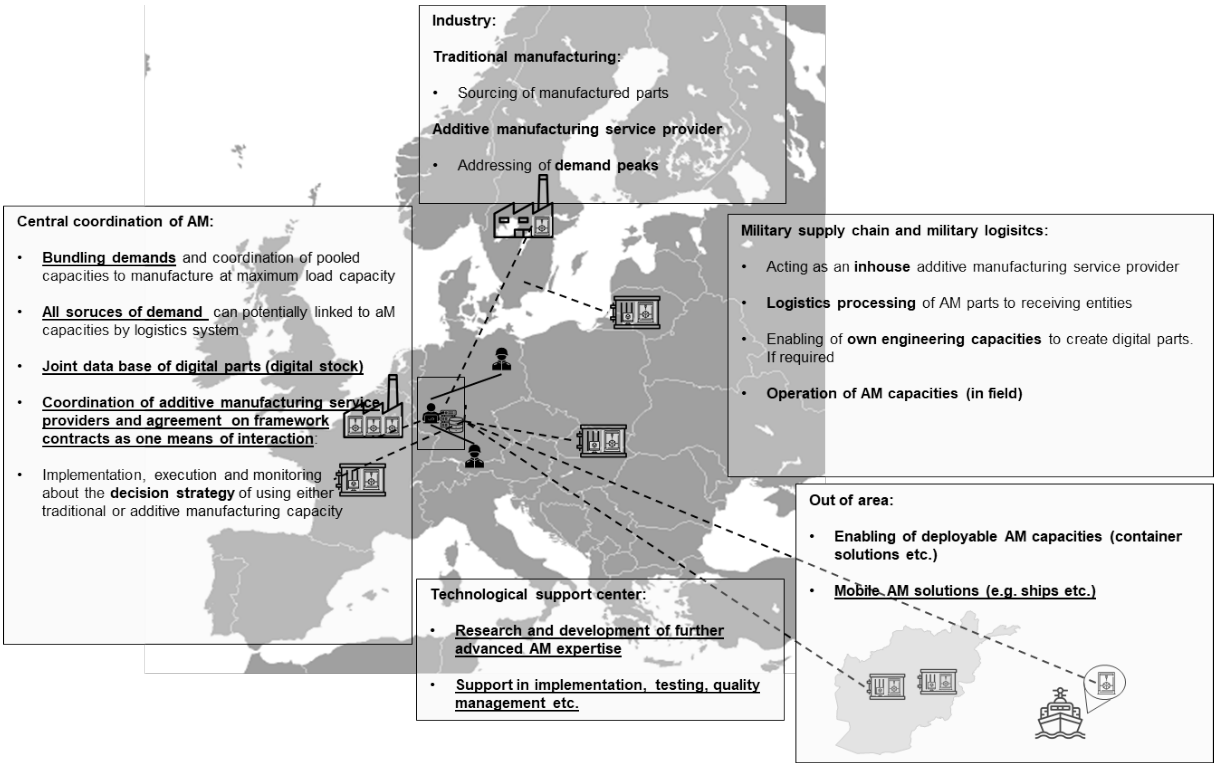
Figure 4. Effect of pooled demand on AM efficiency

7. CONCLUSION: DIGITAL DEFENCE SUPPLY CHAIN FOR EUROPE

This research implies that AM in defence supply chains can be used to increase resilience, but only in parallel with traditional manufacturing. This optimizes efficiency, effectiveness, and supply risk for the Armed Forces. Furthermore, AM must be used in the best case at maximum capacity. As such, a bundling of demand and a centralized use of pooled capacities make sense. Digitally enabled communication of CAD-Data, monitoring of AM capacity status, and print job results would then allow a joint /centralized management. AM capacities require a link to the Armed Forces logistics, but in a pooled capacity system, the "last mile" (within 48hrs delivery) does not require full decentralization on an extreme tactical level.

- All this contributes to increase efficiency and effectiveness of defence supply chains. This research argues that AM in form of a pooled capacity hedging from several AM service providers is beneficial, not the use of single stand-alone AM capacities for single tactical level military consumers. As a result, this research takes into account both technical and application aspects of AM and develops a much more integrated, hybrid approach in three directions: Hybrid in terms of a "hedged" combination of AM and traditional manufacturing technologies to combine the advantages of both of them,
- hybrid in terms of integrating multinational cooperative sourcing solutions, if possible on the long run for all cooperating European Union Armed Forces as well as
- hybrid in terms of integration value added from internal (Armed Forces own capacities) and external (suppliers) sources to an integrated, fully digitalized defence supply chain.

It is strongly recommended to establish a pooled management, to connect all users digitally and logistically to AM capacities and to have a digital library of printable parts and secure lines of communication. Bundling of demand, supply decisions on satisfying it either via AM or TM (hedging), and digitally pooled capacities are key to implement AM in a meaningful and efficient way (see Figure 5). Then, AM improves supply availability and reduces the vulnerability of defence supply chains to disruption risks.



Industry:

Traditional manufacturing:

- Sourcing of manufactured parts

Additive manufacturing service provider

- Addressing of **demand peaks**

Central coordination of AM:

- **Bundling demands** and coordination of pooled capacities to manufacture at maximum load capacity
- **All soruces of demand** can potentially linked to aM capacities by logistics system
- **Joint data base of digital parts (digital stock)**
- **Coordination of additive manufacturing service providers and agreement on framework contracts as one means of interaction**:
- Implementation, execution and monitoring about the **decision strategy** of using either traditional or additive manufacturing capacity

Military supply chain and military logisitcs:

- Acting as an **inhouse** additive manufacturing service provider
- **Logistics processing** of AM parts to receiving entities
- Enabling of **own engineering capacities** to create digital parts. If required
- **Operation of AM capacities (in field)**

Out of area:

- **Enabling of deployable AM capacities (container solutions etc.)**
- **Mobile AM solutions (e.g. ships etc.)**

Technological support center:

- **Research and development of further advanced AM expertise**
- **Support in implementation, testing, quality management etc.**

Figure 5. Vision of an AM supported digital defence supply chain

ACKNOWLEDGEMENTS

This research project – LogSimSan – is funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. Dtec.bw is funded by the European Union – NextGenerationEU.

REFERENCES

[1] Huang, S.H., Liu, P., Mokasdar, A. and Hou, L. (2013) 'Additive manufacturing and its societal impact: a literature review', The International Journal of Advanced Manufacturing Technology, Vol. 67, No. 5 [online] https://doi.org/10.1007/s00170-012-4558-5.

[2] International Organization for Standardization (12.2015) ISO/ASTM 52900:2015 ISO/ASTM 52900:2015, ISO. https://www.iso.org/obp/ui/#iso:std:iso-astm:52900:ed-1:v1:en.

[3] Durach, C.F., Kurpjuweit, S. and Wagner, S.M. (2017) 'The impact of additive manufacturing on supply chains', International Journal of Physical Distribution & Logistics Management, Vol. 47, No. 10 [online] http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=126007907&site=ehost-live.

[4] Meyer, M.M., Glas, A.H. and Eßig, M. (2020b) 'Systematic review of sourcing and 3D printing: make-or-buy decisions in industrial buyer–supplier relationships', Management Review Quarterly [online] https://www.springerprofessional.de/systematic-review-of-sourcing-and-3d-printing-make-or-buy-decisi/18455774.

[5] Clemens, M. (2022) "The Use of Additive Manufacturing in The Defense Sector", available at: https://www.3dnatives.com/en/the-use-additive-manufacturing-defense-sector300620224/#!, accessed: 30.03.2023.

[6] The aviation industry hub (2021) "The "slow revolution" of additive manufacturing within aerospace", available at: https://www.wearefinn.com/topics/posts/the-slow-revolution-of-additive-manufacturing-within-aerospace/ accessed: 30.03.2023.

[7] Rinaldi, M., Caterino, M., Manco, P., Fera, M., & Macchiaroli, R. (2021). The impact of Additive Manufacturing on Supply Chain design: A simulation study. Procedia Computer Science, 180, 446-45.

[8] Valtonen, I., Rautio, S. & Salmi, M. "Capability development in hybrid organizations: enhancing military logistics with additive manufacturing" Prog Addit Manuf 7, pp1037–1052.

[9] Rautio, S., & Valtonen, I. Supporting military maintenance and repair with additive manufacturing. Journal of Military Studies.

[10] Valtonen, I., Rautio, S. and Lehtonen, J.-M. (2022), "Designing resilient military logistics with additive manufacturing", Continuity & Resilience Review, Vol. ahead-of-print, https://doi.org/10.1108/CRR-08-2022-0015

[11] Bundeswehr (2018) „Konzeption der Bundeswehr Konzeption der Bundeswehr 2018, available at: https://www.bmvg.de/de/aktuelles/konzeption-der-bundeswehr-26384, accessed: 30.03.2023, p. 72

[12] BCG-Matrix, u.a. hier: Schawel, C. und Billing F. (2018), BCG-Matrix, Top 100 Management Tools, Springer Gabler, Wiesbaden, S. 41-43

[13] Fisher M.L. (1997), What is the right supply chain for your product?, Harvard Business Review, Nr. 3, S. 105-116

[14] Asbjørnslett, Bjørn Egil, 2009. Assessing the vulnerability of supply chains. In: Zsidisin, G.A., Ritchie, B. (Hrsg.) Supply chain risk: A handbook of assessment, management, and performance, Boston, MA, Springer, S. 15-33.

[15] Meyer, M. M., Glas, A. H., & Eßig, M. (2022). Learning from supply disruptions caused by SARS-CoV-2: use of additive manufacturing as a resilient response for public procurement. Journal of Public Procurement, 22(1), 17-42.

[16] Berman, B. (2012) '3-D printing: The new industrial revolution', Business Horizons, Vol. 55, No. 2 [online] http://www.sciencedirect.com/science/article/pii/S0007681311001790.

[17] Holmström, J. and Partanen, J. (2010) 'Rapid manufacturing in the spare parts supply chain', Journal of Manufacturing Technology Management, Vol. 21, No. 6, pp.687–697.

[18] Baldinger, M. (2016) Supply chain management für additive manufacturing. Konzepte, Werkzeuge und Prozesse für die Zusammenarbeit mit Dienstleistern zur Reduktion der Risiken beim Einstieg in additve Manufacturing, ETH

Zurich [online] https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/114551/eth-48847-02.pdf?sequence=2&isAllowed=y (Accessed 13 June 2019).

[19] Meyer, M. M., Glas, A. H., & Eßig, M. (2022). A Delphi study on the supply risk-mitigating effect of additive manufacturing during SARS-COV-2. Journal of Purchasing and Supply Management, 28(4), 100791.

[20] Markowith, H. (1952). Portfolio selection, Journal of Finance 7 (1), pp77-91.

[21] Oehler, A. & Unser, M. (2001), Finanzwirtschaftliches Risikomanagement, Springer Berlin, Heidelberg, Berlin.

[22] Dadfar, D., Schwartz, F., & Voß, S. (2012). Risk management in global supply chains–Hedging for the big bang. In Transportation & Logistics Management. Proceedings of the 17th International HKSTS Conference, HKSTS, Hong Kong (pp. 159-166).

[23] Hedenstierna, C.P.T., Disney, S.M., Eyers, D.R., Holmström, J., Syntetos, A.A. and Wang, X. (2019) 'Economies of collaboration in build-to-model operations', Journal of Operations Management, Vol. 65, No. 8, pp.753–773.

[24] Attaran, M. (2017). The rise of 3-D printing: The advantages of additive manufacturing over traditional manufacturing. Business horizons, 60(5), 677-688.

Authors

Andreas H. Glas, is Assistant Professor and Managing Director of the Defence Acquisition & Supply Management (DASM) research group at Bundeswehr University Munich. As such he leads a unique research cell focusing on defence armament from a business administration perspective in Germany. His research investigates the buyer-supplier interface and in particular performance-based contracts. He co-edited the Springer book Performance-based Logistics, published a book on military economics, and his articles on the topic have appeared in dedicated defence journals including the Journal of Defense Analytics and Logistics or the Journal of Military Studies. He can be contacted at andreas.glas@unibw.de

Michael Essig, is full professor and head of the Working Field Procurement in the Department of market-oriented supply chains of at Bundeswehr University Munich. This includes the Research Centre for Law and Management of Public Procurement, the Audi Procurement Research Group, and the Research Centre for Defence Acquisition and Supply Management. His peculiar research interest lies in public and even more specific in defence procurement. He published several books on the topic, including teaching books on procurement and supply chain management. He acts as a Co-Editor and reviewer for a number of academic journals. He can be contacted at: michael.essig@unibw.de

GREEN ENERGY RESILIENCE AGAINST MISSILE & DRONE ATTACKS – ECONOMICS OF TARGETING WIND & SOLAR ENERGY

Pedro Gonçalo Rodrigues Soares Barbosa Silva

Abstract

This paper focuses on the Resilience of Solar and Wind energy infrastructure, from an "economics of war" perspective, when faced with the threat of missile and drone attacks. The pertinence of this paper derives not only from the objectives of the European Clean Energy Transition, but additionally from updated energy security concerns related to the targeting of critical energy infrastructure in Ukraine. Estimates of the cost of missile/drone barrages, of SAM systems, and of wind/solar infrastructure were utilized for the cost/benefit analysis, taking into account the attacker's and defender's perspective. This strategy of energy denial, depending on the scenario, could have an estimated cost as low as $5 per kWh denied, for the attacker. Seeing as 1 kWh roughly equals the electricity used by a kitchen oven, this calculation reveals the economic resilience of green energy, and can explain the employment of alternative strategies by an attacking state.

Keywords

Energy Resilience, Energy Transition, Drones, Missiles, SAM Systems.

1. MAIN FINDINGS

- There is no Economic logic in physically targeting or defending Solar energy, since its infrastructure and cost characteristics are a sufficient deterrent.
- Wind turbines, when targeted en mass with drones, are the most economically viable target (between Wind and Solar) for the attacker, but $5 per kWh denied might represent an inefficient cost/benefit relationship.
- The defense of Wind turbines, if targeted, can make economic sense (relative to the cost born by the attacker) but only with the employment of specific UAV-countering, lower cost/less powerful SAM systems.
- The inefficient cost/benefit relationship in physically targeting Solar and Wind farms points to the higher probability of alternative attacks, such as targeting Energy Transmission bottlenecks (i.e. control centres; Inverter/transformer sub-stations; etc.) with either alternative physical or cyber weapons.
- The investment in Solar and Wind energy has robust Strategic and Environmental benefits.

2. EXPLAINING THE USE OF RUSSIAN/IRANIAN AND WESTERN SYSTEMS FOR COST ESTIMATES

The following paper will be heavily influenced by the developments and strategies employed in the Russia-Ukraine War. The strategic targeting of critical energy infrastructure is not novel, but the use of modern drone/missile (defence) systems in this conflict makes an updated review of its cost/benefit analysis a necessity. As such, the following chapters will focus on the offensive and defensive systems in use by both sides in the war in Ukraine, with this list representing the basis for the economic analysis of the aforementioned strategy. The implication of using costs associated with Russian/Iranian missile and drone systems, and the costs associated with western SAM systems permits a cost/benefit analysis more closely aligned with a European Defence perspective. Finally, with the investment in the development of more affordable and flexible SAM systems, and the observable trend of decreased costs of Wind and Solar Energy investments, the cost/benefit estimate for the Defender is expected to be even more optimistic in the future.

3. MISSILES, DRONES, SAM SYSTEMS, AND ASSOCIATED COSTS

3.1. MISSILES AND DRONES EMPLOYED BY ATTACKER

Russia has fired a variety of missiles. Ukrainian made *Kh-55* subsonic cruise missile – some used as decoys for Ukrainian SAM systems, others fitted with modernized warheads – from the 1970's, precision *Kh-101* cruise missiles, as well as sea-based *Kalibr* cruise missiles [ ]. In addition, *Iskander-K* missiles, Iranian short-range ballistic missiles (SRBM), *Kh-59* air-to-surface missiles, *Kh-47M Kinzhal* hypersonic air-launched missiles, missiles launched from *S-300* surface-to-air systems, *KH-31* missiles, *Kh-22* missiles, *3M14 Kalibr, 9K720 Iskander-M* short-range ballistic missiles, *9M723 Iskander-M* ballistic missiles (with multiple decoy capabilities), *9M728 Iskander-K* cruise missile, *Tochka/SS-21 Scarab* mobile short-range ballistic missile, and *Kh-31P* supersonic anti-radiation missile [ ]. Regarding the drones: *Kalashnikov/ZALA KYB* (loitering munition), *Eleron-3SV* (reconnaissance UAV), *Orlan-10* (with electronic warfare/jamming payload capabilities), *Forpost R* (ISR UAV), *Kronshtadt Orion* [ ]; as well as the *HESA Shahed-131* (*Geran-1*, as it is named in the Russian military) and the *Shahed 136* (*Geran-2*) [ ] which have been mainly utilized as less expensive munition for the targeting of Ukrainian energy.

3.2. COST OF MISSILE AND DRONE BARRAGES

The Russian missile barrages usually consist of different combinations of missiles and UAVs, in number and in model. Additionally, barrages between 60 to 100 warheads have been witnessed in Ukraine, leading to an estimated cost of Russian missile barrages ranging from $400-700 million. Supporting this estimate with the costs of Russian missiles, the *Kh-101* missile costs $13 million, *Kh-555* is around $4 million, *3M-54 Kalibr* has a domestic price below $1 million ($6.5 million for export market), *Kh-22* is too close to $1 million with the *Kh-59* and the *Kh-31P* closer to $0.5 million each [ ].

When we analyse the episodes of drone barrages of Iranian *Shaheds* – observable episodes of barrages ranging from 10 to 40 UAVs – we can attempt a calculation of the cost spectrum associated with drone salvos resulting in a range between $200,000 (cost-saving end of spectrum: 10*$20,000) and $2,000,000 (opposite end of cost spectrum: 40*$50,000). Underpinning this estimate, the costs of Iranian/Russian drones and loitering munition barrages: the *Shahed-136* costs an estimate of $20,000 to $50,000, and its sibling, the *Shahed-131*, carries a similar estimated cost of $20,000 to $30,000. Disregarding, solely for a cost comparison, the differences in capabilities between i.e. Russian cruise missiles and i.e. Iranian drones, it is transparent the cost incentives for future drone salvos; even when considering the most expensive scenario of drone barrages against the estimated costs of Russian missile barrages ($400 - $700 million).

3.3. SAM SYSTEMS AND INTERCEPTORS

Focusing on the SAM (surface-to-air missile) systems in use under the Ukrainian military, it has been reported the presence of *S-300 systems* – Kyiv had around 250 of these soviet systems before the invasion – as well as more modern technology, like the German *IRIS-T* – capable of defending an entire city from a variety of threats such as cruise missiles or drones. The US/Norwegian *NASAMS* has been witnessed as, the US-made *Patriot* Systems, the American *Hawk* System – made for low-flying aircraft in the 1950's, but capable of countering the Iranian drone threat – as well as smaller defence systems. The *Avenger, Leopard*, and *Gepard* – respectively, two missile, and one gun based – systems are smaller in scale and more suited for countering UAVs. The Ukrainian military has also in use *MANPADS* (Man-portable air-defense systems). The MANPADS *Starstreak*, *Stinger*, and *Piorum* missile systems are multi-purpose, being effective against UAVs and winged rockets [ ].

3.4. PRICES OF SAM SYSTEMS AND COST OF INTERCEPTORS

Regarding the *S-300* SAM System, in its entirety (detection radar, command-and-control centre, launcher, engagement radar) the system cost rounds up to $115 million, with each interceptor missile costing around $1,000,000. The missiles that are used by *IRIS-T SL* have a price that can reach to $480,000, with the complete battery system costing $140 million. The Norwegian *NASAMS* has a complete cost greater than $180 million, with each interceptor priced up to $1.1 million. The *Patriot* system is one of the more expensive ones, with the *PAC-3* interceptor costing $3.8 million, and the complete system $1.1 billion (radar, control station, power generators, 5-8 launchers, missiles, support vehicles/equipment). This system is considered a theatre-scale SAM system, with its cost and sophistication making it unsuitable for countering lower-tier threats such as drones. Regarding lower cost/capability SAM systems, the Hawk missile system is priced at $15 million per fire unit, with its missiles costing $250,000. The vehicle-mounted AN/TWQ-1 Avenger SAM System used mostly FIM-92 Stinger missiles, which cost up to $40,000 per unit, and depending on the vehicle it is mounted on, the vehicle can cost up to $8 million (i.e. *IM-SHORAD* [Interim Maneuver Short-Range Air Defense] *Stryker*). The *Flakpanzer Gepard* – a German self-propelled anti-aircraft gun (SPAAG) – has revealed itself a cheaper and effective alternative against Iranian drones. The *Vampire* SAM System is a portable system which can be installed in larger vehicles with a cargo bed, making it flexible and more affordable - its missiles have a cost as low as $27,000.

4. COSTS ASSUMPTIONS ASSOCIATED WITH SOLAR AND WIND ENERGY

4.1. COSTS WITH SOLAR ENERGY

With 400Wh panels taken as the standard, and 4.5 peak hours of sunlight as the average of peak sunlight, it will be assumed that each solar panel is capable of producing [ ] [400Wh * 4.5h = 1.8 kWh] per day. In terms of prices of 2019, construction costs for solar generation were $1,796 per kWh [ ]. Seeing as 1.8 kWh per day per solar panel equals 0.075 kWh per panel (divided by 24h), then each solar panel – taking into consideration the calculations are focusing on utility solar farm-related costs, and not rooftop solar panels – each solar panel will have a cost of $135. These numbers will help establish an estimate for costs associated with each solar panel that is destroyed in a drone/missile attack.

Regarding the estimates for the number of damaged solar panels per drone/missile that successfully hits the intended target, this paper will utilize the episode of a Russian missile attack in the Merefa Solar Plant, near Kharkiv, in order to approximate of the expected damage of missile [ ]. Since the model of the two missiles was not found, and 416 solar panels were damaged or destroyed, this paper will from now assume each missile that evades interception represents 208 solar panels that are damaged. In order to estimate the potential damage done by "suicide drone" barrages, this paper will extrapolate from the warheads of Iranian drones (i.e. *HESA Shahed-131*; *HESA Shahed-136*) the explosive damage of a drone attack on solar panels. Respectively, these Iranian drones have a 15kg and 30-50kg warhead. This paper will assume a 50/50 combination of both UAVs in drone barrages, with [(15kg*50%) + (50kg*50%) = 32.5kg] offering the average warhead weigh in a drone barrage (when considering the maximum warhead weight for the *Shahed-136*). This permits the estimation of the radius of damage (assuming a TNT-like explosive type) which is 15 metres, with a 32.5kg warhead. Since the average standardized solar panel is 2m^2, and we assume 50% of the land space in the solar farm is not covered by the solar panels, then we can calculate the approximate number of solar panels affected inside the radius, which will be [(15^2*3.14) * 0.5]/2 = 175 solar panels (damage could be intensified with the use of Steel ball blast fragmentation warhead).

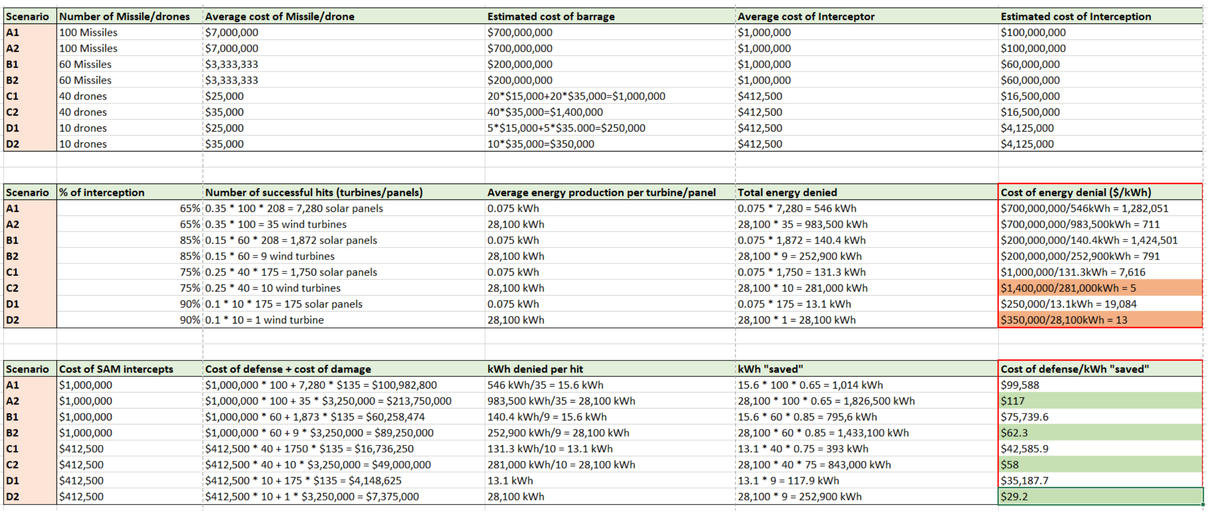
4.2. COSTS WITH WIND ENERGY

This paper will now assume that the average on-shore wind turbine is able to produce 2 - 3 MW, with a cost of $1.3 million per MW, which leads to an average of [(2MW + 3MW)/2] * $1,300,000 = $3,250,000 [ ]. Furthermore, the average wind turbine will generate 28,100 kWh. This paper will not focus on off-shore wind farms since only roughly 7% of wind turbines are off-shore, although it does acknowledge further studied of the topic could bring additional nuances to the resilience/vulnerabilities of Wind energy when confronted with missile and drone threats. The paper will follow with its assumptions, by assuming missile barrages would witness a 100% success rate in hitting wind turbines (in a scenario where the warheads are not intercepted) because the average dimensions of the wind turbine's nacelle are big enough for a critical hit [i.e. 20m x 7m]). Suicide drones would see the same assumption, with the accuracy of the Iranian drones in the battlefield having shown to be extremely precise. The infrastructure of the Wind turbine is much more robust than Solar panels, with steel and concrete offering a strong outer shell. The mass of the whole turbine can reach well above 500,000kg, therefore this paper will exclude the use of the lighter Iranian UAV in the hypothetical drone barrage, and assume that in case the Shahed-136 drone would not be capable of destructive damage, it would nevertheless force the turbine to cease operating for maintenance/repairs/check-up purposes.

5. ESTABLISHING SCENARIOS FOR CALCULATIONS AND THEIR ASSUMPTIONS

5.1. ESTABLISHING 8 DIFFERENT SCENARIOS

- *Scenario A1:* missile barrage consisting of 100 projectiles, costing $700 million, with an interception rate of 65%. The barrage targeting Solar Farms.
- *Scenario A2:* similar to A1 but the targets are onshore wind turbines.
- *Scenario B1:* smaller missile barrage of 60 missiles, with a cost of $200 million, with an interception rate of 85%, targeting solar farms.
- *Scenario B2:* similar to B1, but the targets are onshore wind turbines.
- *Scenario C1:* drone salvo of 40 Shahed drones (combination of 50% -*131* and 50% -*136*), witnessing an interception rate of 75%, targeting solar farms.
- *Scenario C2:* drone salvo of 40 Shahed drones (100% -*136*), interception rate of 75%, targeting onshore wind farms.
- *Scenario D1:* barrage of 10 Shahed drones (combination of 50% -*131* and 50% -*136*) attack solar farm, witnessing an interception rate of 90%
- *Scenario D2:* barrage of 10 Shahed drones (100% -*136*), interception rate of 90%, targeting onshore wind farm.



Scenario	Number of Missile/drones	Average cost of Missile/drone	Estimated cost of barrage	Average cost of Interceptor	Estimated cost of Interception
A1	100 Missiles	$7,000,000	$700,000,000	$1,000,000	$100,000,000
A2	100 Missiles	$7,000,000	$700,000,000	$1,000,000	$100,000,000
B1	60 Missiles	$3,333,333	$200,000,000	$1,000,000	$60,000,000
B2	60 Missiles	$3,333,333	$200,000,000	$1,000,000	$60,000,000
C1	40 drones	$25,000	20*$15,000+20*$35,000=$1,000,000	$412,500	$16,500,000
C2	40 drones	$35,000	40*$35,000=$1,400,000	$412,500	$16,500,000
D1	10 drones	$25,000	5*$15,000+5*$35.000=$250,000	$412,500	$4,125,000
D2	10 drones	$35,000	10*$35,000=$350,000	$412,500	$4,125,000

Scenario	% of interception	Number of successful hits (turbines/panels)	Average energy production per turbine/panel	Total energy denied	Cost of energy denial ($/kWh)
A1	65%	0.35 * 100 * 208 = 7,280 solar panels	0.075 kWh	0.075 * 7,280 = 546 kWh	$700,000,000/546kWh = 1,282,051
A2	65%	0.35 * 100 = 35 wind turbines	28,100 kWh	28,100 * 35 = 983,500 kWh	$700,000,000/983,500kWh = 711
B1	85%	0.15 * 60 * 208 = 1,872 solar panels	0.075 kWh	0.075 * 1,872 = 140.4 kWh	$200,000,000/140.4kWh = 1,424,501
B2	85%	0.15 * 60 = 9 wind turbines	28,100 kWh	28,100 * 9 = 252,900 kWh	$200,000,000/252,900kWh = 791
C1	75%	0.25 * 40 * 175 = 1,750 solar panels	0.075 kWh	0.075 * 1,750 = 131.3 kWh	$1,000,000/131.3kWh = 7,616
C2	75%	0.25 * 40 = 10 wind turbines	28,100 kWh	28,100 * 10 = 281,000 kWh	$1,400,000/281,000kWh = 5
D1	90%	0.1 * 10 * 175 = 175 solar panels	0.075 kWh	0.075 * 175 = 13.1 kWh	$250,000/13.1kWh = 19,084
D2	90%	0.1 * 10 = 1 wind turbine	28,100 kWh	28,100 * 1 = 28,100 kWh	$350,000/28,100kWh = 13

Scenario	Cost of SAM intercepts	Cost of defense + cost of damage	kWh denied per hit	kWh "saved"	Cost of defense/kWh "saved"
A1	$1,000,000	$1,000,000 * 100 + 7,280 * $135 = $100,982,800	546 kWh/35 = 15.6 kWh	15.6 * 100 * 0.65 = 1,014 kWh	$99,588
A2	$1,000,000	$1,000,000 * 100 + 35 * $3,250,000 = $213,750,000	983,500 kWh/35 = 28,100 kWh	28,100 * 100 * 0.65 = 1,826,500 kWh	$117
B1	$1,000,000	$1,000,000 * 60 + 1,873 * $135 = $60,258,474	140.4 kWh/9 = 15.6 kWh	15.6 * 60 * 0.85 = 795,6 kWh	$75,739.6
B2	$1,000,000	$1,000,000 * 60 + 9 * $3,250,000 = $89,250,000	252,900 kWh/9 = 28,100 kWh	28,100 * 60 * 0.85 = 1,433,100 kWh	$62.3
C1	$412,500	$412,500 * 40 + 1750 * $135 = $16,736,250	131.3 kWh/10 = 13.1 kWh	13.1 * 40 * 0.75 = 393 kWh	$42,585.9
C2	$412,500	$412,500 * 40 + 10 * $3,250,000 = $49,000,000	281,000 kWh/10 = 28,100 kWh	28,100 * 40 * 75 = 843,000 kWh	$58
D1	$412,500	$412,500 * 10 + 175 * $135 = $4,148,625	13.1 kWh	13.1 * 9 = 117.9 kWh	$35,187.7
D2	$412,500	$412,500 * 10 + 1 * $3,250,000 = $7,375,000	28,100 kWh	28,100 * 9 = 252,900 kWh	$29.2

Figure 1. Table with Economic Cost Calculus

5.2. ASSUMPTIONS SUSTAINING THE COST ANALYSIS

Many assumptions and simplifications had to be made to conduct an analysis in a more linear manner. The bigger missile barrage was imagined as a more expensive salvo, i.e. integrating the *Kh-101* missiles, while the more "conservative" barrage of 60 missiles was established as a more affordable option – hence the cost disparity between $200 and $700 million. It was decided to separate the attacks on wind farms from the attacks on solar panels, since it permits an isolation of costs associated with specific attacks, and a review of the particular resilience characteristics of each energy source. The separation of the drones from the missiles, yet again a phenomenon admittedly far away from reality, permits a better view into the "Economics of War" phenomena, where inexpensive loitering munitions add pressure to the expensive SAM systems. Another phenomenon integrated into the scenarios, is the fact that the more missiles/drones in a barrage the more difficult it will be to intercept them all; meaning that the paper concedes a measure of additional success with the strategy of increased swarming. After deciding on the ranges of costs for the Russian missile barrages, it was decided that for the interceptors of missile barrages, there will be an assumption of $1,000,000 per interceptor – after a review of the cost of each SAM system most suited for countering missiles – and the practice of only one interceptor per missile/drone. For the Drone barrages, it will be considered a tripartite combination of $1 million interceptors, as well as $250,000 and $40,000. [33% * $1,000,000 + 33% * $250,000 * 33% * $40,000 = $412,500]. This is explained by the insufficient amount of inexpensive SAM systems capable of intercepting UAVs; thus, for a more realistic scenario, the defending part will be obligated to use more expensive SAM systems to intercept cheaper drones. The interception percentages are also a simplification, since they do not realistically represent the situation in all of Ukraine. The biggest cities, i.e. Kyiv, see interception rates way above the national average; while the more rural areas in the interior usually suffer interception rates below 50%. The majority of Wind and Solar farms in Ukraine are situated in the south of Ukraine, pointing to a proximity not only to rural areas, but also to areas directly connected to the battle (more potential for damage from other sources). Finally, the simplifications are merely a starting point for a structured thought process and calculation model. Nevertheless, it is the belief of the author that the simplifications abovementioned do not deny the model from aiding in potentially realistic scenario building, being mainly useful for rough initial cost comparisons.

6. CONCLUSIONS FROM THE TABLE:

Wind Power electricity generation is much more concentrated than Solar Energy generation, and therefore is more vulnerable to any type of physical attack. Associated with this, it is observable in the "middle row" that the economic cost per kWh denied to the defending party (Ceteris Paribus, under certain circumstances) – scenario C2 of 40 Shahed-136 focusing on the "average" wind turbine, with only 75% of interception – for the attacker can reach comparably low levels = $5 per kWh denied. Another point is that, because of cost dynamics between drones, cruise missiles, SAM systems, etc. when observing the comparison of costs between the defensive and offensive posture, the disproportionate economic pressures associated with "Economics of War" make themselves very clear = Cost of Defence > Cost of Attack. Even with an assumption regarding an equal tripartite combination with less advanced/costly SAM systems, and a majority of less expensive SAM systems; the cost becomes prohibitive very fast. Finally, in the "bottom row" there is calculated the cost of defence, in terms of "kWh saved" from the missiles or drone barrage. It points to the economic logic of not allocating SAM systems for the defence of Solar panels, and to the argument that the defence of Wind turbines can make economic sense only with the employment of UAV-countering (lower cost/less powerful) SAM systems. Finally, these cost/benefit relationships do not translate into the inexistence of threats to Wind and Solar energy infrastructure; in all likelihood, the tactics and weapons employed will just have to change – i.e. physical attack on energy transmission bottleneck (control centres; Inverter/transformer sub-stations, etc.), or cyberattacks.

7. CONCLUSIVE COMMENTS ON RESILIENCE OF SOLAR AND ENERGY POWER

7.1. COMMENT ON SOLAR ENERGY RESILIENCE

There is no Economic logic in physically targeting Solar Energy, the characteristics of its production are enough to deter an attack. Solar PVs are modular, meaning that the damaged components can be separated from the intact panels (isolating the damage) and the string inverters connecting the panels can be diverted, reconnecting only the surviving modules to the electricity grid. This characteristic guarantees a faster recovery and partial power generation, while the remaining damaged solar PVs can be repaired [ ]. Solar PVs are increasingly inexpensive to purchase and install, and more versatile. The LCOE of Solar PVs has consistently decreased since the last decade, with the number of projects for utility scale solar farms, community scale solar farms, unit/family scale; increasing. The resulting trend is more geographically spread units, scale diversification and minimization, and differentiation of customers (i.e. family unit, community, power company) – translating in higher strategic resilience of Solar Energy. With the unit price of each solar PV (estimate of around $1000 including installation and maintenance) being a fraction of the cheapest loitering munitions, the "Economics of War" dynamic is reversed, with the attacker facing higher costs. The investment in a "smart grid" would galvanize the resilience potential of Solar energy, not only with an increase in energy efficiency, but with the potential of isolating communities from the damage of bigger-scale attacks/power outages. Attention needs to be paid to the potential for the use of cluster munition against the fragile Solar Panels (increasing damage radius), or the use of Incendiary munitions depending on the surface of the Solar farm. Cyberattacks is a very likely threat, associated with a bigger integration of the energy grid with internet-of-things-type services, or with the expansion of the "smart grid" concept.

7.2. COMMENT ON WIND ENERGY RESILIENCE

Wind turbines, although most likely not high on the target priority list of attacking countries, are nevertheless vulnerable. The potential for growth in investment into off-shore Wind turbines is high, and it brings about difficulties in its physical defence. SAM systems in maritime environments are a more costly and complex operation, the options for attacking such infrastructure multiply, as well as the fact that off-shore Wind turbines are usually bigger in dimension and power-generation. This culminates in a more inviting context for an attacking state. The cyber threat scenario for Wind turbines is just as propitious, if not more than Solar Energy, since the concentration of power-generation in a single energy transmission bottleneck is much greater.

Bibliography

[1] Santora, M. (2022, December 12). Russia is using old Ukrainian missiles against Ukraine, general says. The New York Times. Retrieved January 23, 2023, from https://www.nytimes.com/2022/12/12/world/europe/russia-ukraine-missiles.html

[2] Ukrainian War updates. Missile Defense Advocacy Alliance. (2023, January 19). Retrieved January 23, 2023, from https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/ukrainian-war-updates/

[3] Lowther, A., & Siddiki, M. K. (2022). Combat Drones in Ukraine. AIR & SPACE OPERATIONS REVIEW. Retrieved January 23, 2023, from https://www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-1_Number-4/Lowther.pdf?source=GovD

[4] Almeida, A., & Knights, M. (2022, November 10). What Iran's drones in Ukraine mean for the future of war. The Washington Institute. Retrieved January 23, 2023, from https://www.washingtoninstitute.org/policy-analysis/what-irans-drones-ukraine-mean-future-war

[5] Тарасовський, Ю., & Ланда, В. (2022, December 6). Росіяни 5 грудня випустили по Україні ракет на $400–500 млн. Оцінка Forbes. Масований ракетний обстріл 5 грудня коштував Росії $400-500 млн. Оцінка Forbes - Forbes.ua. Retrieved January 23, 2023, from https://forbes.ua/news/rosiyani-5-grudnya-vipustili-raket-po-ukraini-na-400-500-mln-otsinka-forbes-06122022-10275

[6] Foltynova, K. (2022, December 27). Protecting the skies: How does Ukraine defend against Russian missiles? RadioFreeEurope/RadioLiberty. Retrieved January 23, 2023, from https://www.rferl.org/a/ukraine-missile-defense-weapons-charts-russia/32192132.html

[7] Ost, I. (2022, September 19). How much energy does a solar panel produce? Solar.com. Retrieved January 23, 2023, from https://www.solar.com/learn/how-much-energy-does-a-solar-panel-produce/

[8] Average U.S. construction costs for solar generation continued to fall in 2019. Homepage - U.S. Energy Information Administration (EIA). (2021, July 16). Retrieved January 23, 2023, from https://www.eia.gov/todayinenergy/detail.php?id=48736

[9] Ukrainian solar plant partly resumes operations after bombing. pv magazine International. (2022, June 2). Retrieved January 23, 2023, from https://www.pv-magazine.com/2022/06/02/ukrainian-solar-plant-partly-resumes-operations-after-bombing/

[10] Blewett, D. (2021, December 20). Wind turbine cost: Worth the million-Dollar price in 2022? Weather Guard Lightning Tech. Retrieved January 23, 2023, from https://weatherguardwind.com/how-much-does-wind-turbine-cost-worth-it/

[11] Sensiba, J. (2022, June 22). Solar power plants are more missile resistant. CleanTechnica. Retrieved January 23, 2023, from https://cleantechnica.com/2022/06/22/solar-power-plants-are-more-missile-resistant/

SWARMING: A DISRUPTIVE, GAME CHANGING TECHNOLOGY FOR DEFENSE APPLICATIONS

Vaios Lappas[1], Ioannis Daramouskas[2], Nicki Patrinopoulou[2], Dimitris Meimetis[2], Vassilis Kostopoulos[2]

Abstract

Swarming is a disruptive and game changing technology which is based on the coordinated use of multiple unmanned vehicles operating in multiple domains (air, ground, sea, space). The development of new microelectronics, guidance and navigation, sensors and AI techniques have enabled the use of low cost, miniature unmanned robots to perform challenging tasks. When combined with novel decision making, target tracking , communications technologies and algorithms, swarms can create a very disruptive impact in the battlefield with applications ranging from persistent and undetected monitoring to delivering crucial defence capabilities such as loitering ammunitions. The paper describes European activities in swarming and provides insight on the game-changing impact it can have for the defence and civilian sectors.

Keywords

Unmanned Vehicles (UxV), autonomy, decision making, target tracking, guidance and control, sensor fusion, intelligence, surveillance and reconnaissance (ISR), unmanned traffic management (UTM).

1. INTRODUCTION

Swarms of unmanned vehicles (UxVs)[3] consist of a large number of heterogeneous unmanned vehicles (air, land, sea) operating as an intelligent group of autonomous 'systems' with decision making, target tracking, guidance and control, sensor fusion and command capabilities which operate as a single intelligent group (autonomous system). Swarms of unmanned vehicles, operating as swarms of bees or birds, if designed with the necessary intelligence and autonomy by using developments in the areas of robotics, artificial intelligence (AI), communications, guidance and control, sensor fusion, aerospace and unmanned traffic management (UTM), can create disruptive, game changing capabilities for the defence sector combining the strengths of numbers and intelligent, smart technologies. A swarm of unmanned vehicles can create unprecedented capabilities which can enhance Europe's safety, defence capabilities and at the same time create disruptive impact on other non-defence sectors such as urban mobility, UTM, autonomous driving or robotics. In the defence context, combined use of unmanned vehicles can limit human risk/exposure in dangerous environments, allow dull and dirty military operations to occur such as the persistent monitoring of large areas (e.g. Mediterranean Sea, European borders) or even be used to confuse and overwhelm adversaries in future military scenarios. Figure 1 shows a multi-domain (air-space-ground-sea-space) concept of a swarm of unmanned systems used to protect and provide persistent surveillance for a high value asset such as a military camp/installation, first proposed in the EDA R&D pilot project EuroSWARM in 2016[4].

[1] National & Kapodistrian University of Athens, Department of Aerospace Science and Technology, Athens, Greece valappas@aerospace.uoa.gr

[2] University of Patras, Department of Mechanical Engineering & Aeronautics, Rio, Greece

[3] X denotes the air, ground and sea operational areas of unmanned vehicles

[4] www.aml.euroswarm.upatras.gr

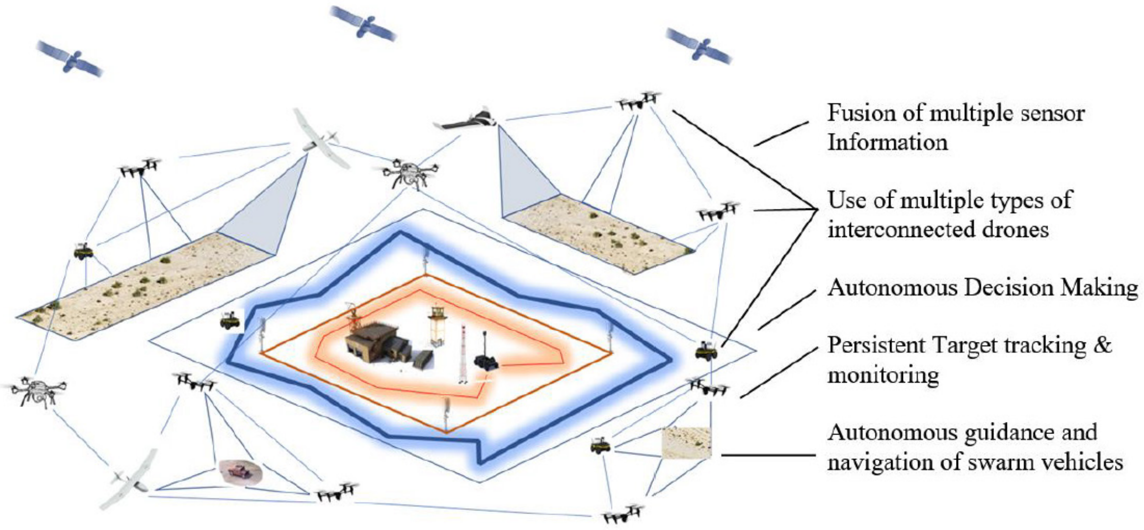

Fusion of multiple sensor Information
Use of multiple types of interconnected drones
Autonomous Decision Making
Persistent Target tracking & monitoring
Autonomous guidance and navigation of swarm vehicles

Figure 1: Multi-domain Swarming Concept (Air-space-ground-surface)

2. SWARMING TECHNOLOGY

Unmanned vehicle (UV) swarms are groups of autonomous or semi-autonomous vehicles that collaborate to achieve a common purpose. UV swarms could be utilised in defence applications for a variety of missions such as reconnaissance, surveillance, target acquisition, and striking operations. This section looks at three main characteristics of swarms for defence applications: (1) the most crucial capabilities and technologies that enable the development of efficient swarms are summarised, (2) the main architecture schemas used when designing a swarm, and (3) some of the operation types often combined to describe a swarm's mission for defence applications. When it comes to swarm design, there are four major technology modules that must be considered for defence applications [1]. Each module serves a very important role for swarm performance and robustness ranging from perception capabilities to swarm communication protocols [2] and routing [3].

1. Perception: Perception capabilities are essential for the success of swarms of unmanned vehicles. Perception enables the swarm to sense and understand the environment it is operating in, detect obstacles, identify targets, and maintain situational awareness. Effective perception capabilities enable the swarm to operate in complex and dynamic environments and perform a wide range of complex tasks with great efficiency. Machine learning and artificial intelligence techniques can enhance these capabilities and through sensor fusion a swarm can achieve situational awareness at a level not possible before.
2. Task allocation and decision-making: Task allocation and independent decision making are critical for the success of swarms of vehicles. Efficient task allocation ensures that each robot is assigned a specific task that aligns with its capabilities, thus optimising the use of available resources. Swarms can compensate for the failure of one or more robots, and task allocation helps to distribute decision making, enabling the swarm to quickly adapt to changing circumstances. Task allocation also facilitates adaptability, scalability, and faster decision making, making swarms more effective in dynamic and uncertain environments. A swarm is capable of taking better decisions through seamless data exchange between the robots of the swarm. This enables efficient use of resources, increase in robustness and fault tolerance, improved adaptability and greatly enhanced scalability.
3. Path planning and deconfliction: When it comes to swarms, a large number of robots is to be expected. This makes path planning and deconfliction methods crucial for efficient and safe swarm manipulation. The goal of path planning in swarms is to find an optimal path for each robot to reach its destination while avoiding obstacles and minimising the time and energy required. Deconfliction ensures that robots do not collide with each other, allowing each robot to complete its task successfully. For example, in a surveillance mission, path

planning can optimise the routes of the robots to minimise overlap and increase coverage area. Path planning and deconfliction can be achieved using a variety of techniques, including centralised and decentralised approaches. Centralised approaches involve a single entity planning and coordinating the paths of all the robots in the swarm. Decentralised approaches, on the other hand, involve each robot making its own path planning decisions based on local information.

4. Communications: A swarm operates optimally when communication between the robots is seamless and robust. Through sensor fusion a swarm can provide information with higher certainty and resolution. Effective communication protocols enable robots to share information such as their location, status, and task assignments, while routing would be responsible for finding the best path for information to travel between robots. This enables the swarm to operate cohesively, coordinate actions, and share information in real-time. Communication protocols and routing can be achieved using various techniques, such as ad hoc networking, mesh networking, and multi-hop routing. Ad hoc networking allows robots to communicate directly with each other without the need for a fixed infrastructure, while mesh networking enables robots to form a network with redundant paths for communication. Multi-hop routing involves passing information from one robot to another until it reaches its destination, enabling communication over longer distances.

Unmanned vehicle swarms are utilising communication protocols to exchange information, and the protocol is determined by the mission's specific requirements as well as the swarm's features [4]. There are three main architectural approaches that can be used to design swarms of unmanned vehicles for defense applications, including:

1. Centralised Architecture: In this approach, the operations of all the vehicles in the swarm are coordinated by a single central entity, such as a ground control station. The central entity communicates with the agents of the swarm and collects data, process the data, and makes informed decisions. This approach is suitable for small-scale swarms and simple missions.
2. Decentralised Architecture: In this approach, there is no central entity, and each vehicle in the swarm operates independently, making decisions based on local information and communicating with its information with neighbouring vehicles. This approach is suitable for large-scale swarms and complex missions.
3. Hybrid Architecture: This approach combines the strengths of both centralised and decentralised architectures. In this approach, there is a central entity that provides high-level guidance to the unmanned vehicles, while each of them is equipped with local decision-making capabilities.

Swarms of unmanned vehicles present a plethora of military applications and are capable of conducting various different missions. Some key examples of operation types of autonomous swarms are identified here. The presented operation can be combined to create a series of missions.

1. Area coverage: In an area coverage operation the swarm is tasks to scan a given field, utilising the sensors the vehicles are equipped with. In most cases area coverage is desired to be full and the area must be scanned completely. A common approach for the multi-vehicle area coverage problem includes dividing the area of interest into a set of subareas using a decomposition technique and assigning each subarea to one vehicle. For heterogeneous swarms the sensors' range, the vehicles mobility and battery autonomy must be taken into account during the area decomposition to improve the system's efficiency [5]. After each vehicle is assigned a subarea, the vehicles plan their path independently within their regions. A survey of coverage path planning methods is presented in [6], summarising the most common methods for 2D, 3D and multi-vehicle area coverage.
2. Full and persistent area coverage: Full and persistent area coverage requires the swarm to be deployed in such a manner to provide sensor coverage of the entire given area over the whole mission duration. The vehicles of the swarm shall create a formation considering the range of their sensors and possible environment characteristics (e.g., obstacles or areas of occlusion). The vehicles are deployed in a static formation, or in a dynamic formation in case the area characteristics or the desired monitored area evolve over time [5]. The main objective is to design a formation pattern that achieves full static coverage with the minimum number of vehicles.
3. Area search: In area search operations the swam is typically tasked to find specific target sin an area of interest. In this operation a complete or full coverage of the area is not required. The swarm must explore the area

with the objective of identifying the target sin minimum time. The vehicles must cooperate through the duration of the mission and they use online decision-making and path planning techniques to improve the system's performance based on their perception of the environment and the behaviour of other vehicles of the swarm. Area search algorithm can be adjusted to consider probabilities of targets' distributions. Bio-inspired swarm algorithm have attracted the interest of the scientific community for area search operations [7], [8].

4. Area surveillance: Area surveillance operations require the swarm to persistently monitor a given area. Area surveillance is often used for patrolling, monitoring, detections of pop-up or dynamic threats and border security. The objective is usually defined to minimise the maximum age (i.e., the time elapsed since last visit) of regions over long time [9].
5. Target tracking: Commonly a target tracking operation involves one target and one vehicle. The scope of the vehicle is to online plan its path based on its sensory data and its estimation of the target's location and in some cases the predicted behaviour or future location of the target [10]. The vehicle must guide itself to follow constantly the target. With the introduction of swarming capabilities, the target tracking problem can be augmented into a multi-vehicle problem, tracking a single [11] or multiple targets [12].

Overall, the design of swarms for defence applications requires a careful consideration of several factors, including mission requirements, swarm size, communication capabilities, and computational resources.

3. SWARMING PROJECTS AND APPLICATIONS

3.1 EUROSWARM

The EuroSWARM [13] project (Developing technology for UAV swarms in defence applications) was a European Defence Agency project, that was held in November 2016-November 2017 with a consortium consisting of 4 partners from Greece, UK, France and Sweden. The project's key techniques, including static sensor network design, mobile sensor tasking, and information fusion, enable the development of novel algorithms for use in commercially available unmanned vehicles. These algorithms offer low computational power requirements, flexibility, and reconfigurability. In Figure 2, the project's architecture and modules used are presented. The task allocation algorithm based on the greedily excluding technique ensures near-optimal task allocation in real-time, allowing effective swarm control in rapidly changing environments. Enhanced situational awareness is achieved through UAV aerial sensing, a general framework for autonomous behaviour monitoring, and trajectory analysis tools. Sensor fusion technology and decentralized tracking algorithms support automatic target detection and tracking, increasing system reliability and fault tolerance. A reactive and distributed cooperative guidance law is designed for the mobile vehicles, addressing the mission and safety objectives, and interactions between the vehicles and the static sensor network. The practical demonstration of these swarm technologies in a scaled outdoor environment validates the effectiveness of these algorithms and techniques for persistent monitoring in military and law enforcement applications.

The practical demonstration combined all swarm technologies presented in earlier sections, simulated, and validated in a scaled outdoor environment. Due to time and budget constraints, the testing area was limited in size, and the unmanned platforms used to form a swarm of robots were based on COTS systems available in the market. The main objectives of the practical demonstration were to set up the demonstration environment, communications network, and test the swarm functionalities for a persistent monitoring scenario. Multiple combinations of agents, types of vehicles, and number of targets were implemented to assess both homogeneous (same type of vehicle/sensors) and heterogeneous vehicles (optical/IR sensors, fixed wing/quadrotor UAVs).

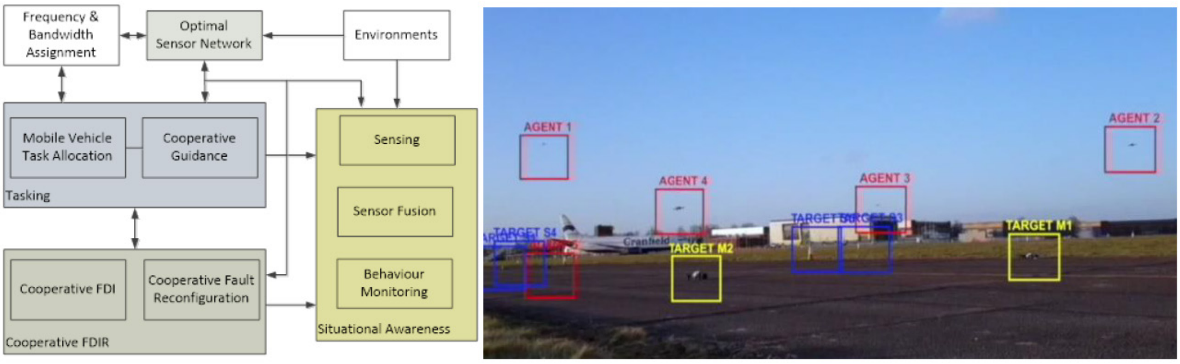


Figure 2. EuroSWARM Architecture2 [13]

3.2 LOW OBSERVABLE TACTICAL UNMANNED AIR SYSTEM - LOTUS

The LOTUS project (Low Observable Tactical Unmanned air System) is an EDIDP project with a consortium consisting of 9 partners from Greece and Cyprus with an additional 2 partners from Spain and the Netherlands. The project kicked off in December of 2020 with a duration of 45 months and is led by Intracom Defense. Through the LOTUS project, a state-of-the-art unmanned aerial vehicle (UAV) system is designed for tactical air reconnaissance and surveillance missions. It boasts several key characteristics, including stealth properties to hide from enemy forces, stand-off operational capabilities, airworthiness, and interoperability based on NATO standards, as well as reliable communications with cybersecurity in mind. Additionally, the system has an extensive adoption of artificial intelligence, ensuring that it can execute complex missions with a high degree of accuracy. The mothership, which is equipped with multiple ISR sensors, is designed for low observability and high endurance and incorporates a self-protection system against enemy threats. It can deploy four tube-launched, foldable-wing drones, which have advanced autonomy features, making them capable of executing complex ISR missions. Together, the mothership and the drones form a powerful swarm that can operate seamlessly, providing critical intelligence and surveillance data to decision-makers on the ground. In Figure 3, the intelligent task allocation (left) and cooperative coverage (right) of a ground target is executed through swarm algorithms developed by the University of Patras.

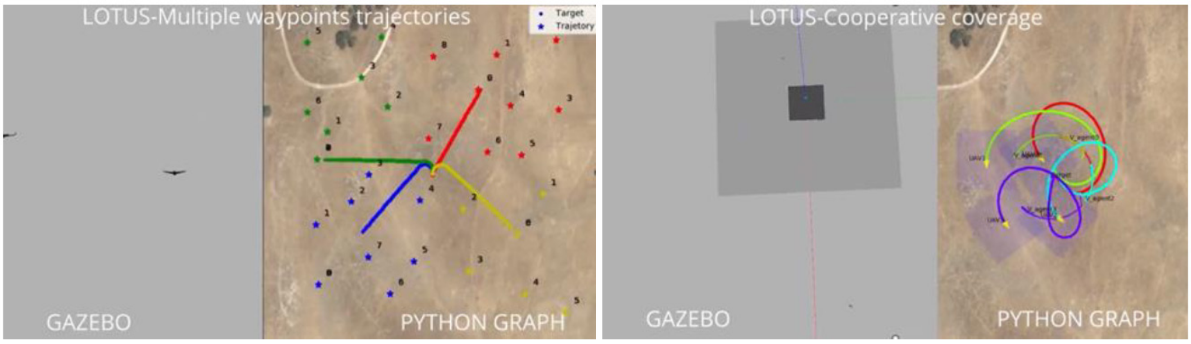

LOTUS-Multiple waypoints trajectories
Target
Trajetory
GAZEBO
PYTHON GRAPH
LOTUS-Cooperative coverage
GAZEBO
PYTHON GRAPH

Figure 3: Operation examples of a UAV swarm in the LOTUS project

3.3 AUTONOMOUS, RECONFIGURABLE SWARMS OF UNMANNED VEHICLES FOR DEFENSE APPLICATIONS - ACHILLES

The ACHILLES project (Autonomous, Reconfigurable Swarms of Unmanned Vehicles for Defense Applications) is an EDA project with a consortium including Greek and German industry and universities.

The project kicked off in January of 2023 and is led by the University of Patras and involved the industry (ATOS, DroniQ, Scytalys, Intracom Defense) and academia (University of Patras, Technische Hochschule Ingolstadt and University of Athens). The project aims to advance the development and use of unmanned swarms for defence applications by elevating the TRL of autonomous, reconfigurable swarms of unmanned vehicle for specific defence missions, and to demonstrate the capabilities and readiness level of swarms for persistent monitoring in defence. The multiple benefits and potential application of swarms of unmanned vehicles have been recognised and have been an inspiration for the ACHILLES project. Recent scientific and technological advancements have enabled unmanned vehicles to autonomously gather crucial data to enhance the situational awareness picture. Scalable, autonomous, and reconfigurable swarms allow for highly efficient agent coordination and are very adaptable to failure events (e.g., the loss of an agent). The expected project's outcomes and innovations contain the formation of new swarming capabilities and methodologies of UAVs integration into military and civil airspace in a safe and efficient manner. The generated capabilities are anticipated to support the maturation and validation of systems and technologies based on swarms of unmanned vehicles.

3.4 CONVOY OPERATIONS WITH MANNED-UNMANNED SYSTEMS - COMMANDS

The COMMANDS project (Convoy Operations with Manned-unManneD Systems) is and EDF project with a consortium consisting of 21 partners from 10 member states. The project kicked off in December of 2022 and is led by Sener Aerospace and Defence with a 3-year execution timeframe along with the support of seven Ministries of Defence which have provided common requirements. The COMMANDS project aims to develop Through Life Capabilities (TLC) for agile, intelligent and cooperative Manned and Unmanned Systems. Several modular systems will be part of this project with swarm capabilities through seamless functional services and data exchange. Manned and unmanned ground vehicles along with UAVs will be part of this system. The project will de-risk and exploit technologies to address the roadmap of self-reliant EU Defence TLC sustainable development. The results will upgrade current ground vehicles and be integrated into future vehicles. The Technology Demonstrator Programme includes both a laboratory and a real scenario Mobile Demonstrator focused on a Last Kilometre Re-supply Convoy with Force Protection.

3.5 UNMANNED TRAFFIC MANAGEMENT: EURODRONE & METROPOLIS 2

Swarming technologies are being used for the civilian sector in various areas including autonomous driving, unmanned traffic management (UTM) and urban mobility. EuroDRONE and Metropolis 2 are EU SESAR funded activities which have demonstrated the successful practical implementation of swarming/autonomy technology for the safe operation of UAVs in civilian airspace with significant commercial applications in logistics, security, medical cargo and precision agriculture [14]. EuroDRONE was one of Europe's first UTM test centres developed and coordinated by the University of Patras (2019-2021).

4. IMPACT

Swarm technology enables a large number of drones to become highly interconnected, with the ability to efficiently plan and allocate mission objectives, make coordinated tactical decisions, and collaboratively react to a dynamic environment with minimal supervision whilst making recommendations to human operators. As swarm technologies mature, the use of swarm military technology is inevitable. Many believe swarm development compares to the development of precision-guided weapons, tested and refined through the 1970s and 1980s, but only coming into their own during the first Gulf War of the early 1990s. The use of swarms can make the use of manned defence systems obsolete for simple, low/medium level, monitoring, surveillance defence scenarios/tasks and compliment attack systems which will distract or constrain enemy forces. Single unit unmanned vehicles operated remotely, such as UAVs will gradually become obsolete in the next decades, as unmanned systems in air, ground, sea will be able to deploy multiple vehicles and operate as swarms, thus extending the range, surveillance, ISTAR and attack capabilities for various defence missions.

Swarming Innovations and Impact	
Disruptive impact in a defence context	Swarms of heterogeneous unmanned vehicles in large numbers (10-100s) operating as intelligent unit can be used for dirty, dangerous and dull missions (persistent monitoring) or to disrupt adversaries (attack of enemy strategic locations/assets) while reducing human risk and cost. Swarms can be a unique defence capability which currently does not exist and is at a low technology readiness level (<3).
Radical vision	Swarms of unmanned vehicles are the epitome or a radical vision, enabling new European defence capabilities and creating a new paradigm for unmanned/ autonomous systems and defence. swarming capitalises on previous EU/NATO defence R&D (EUROSWARM, ACHILLES, COMMANDS) and H2020 activities (EuroDRONE) in the areas of UTM, robotics, sensors, autonomy, UAVs to create a high risk/high gain capability (swarming).
Breakthrough technological target	Using swarms of hundreds of unmanned systems in air, land or sea in the future will create a novel, ambitious capability, and breakthrough. The use of coordinated multiples of agents of UxVs can disrupt military doctrine and operations as shown already in the Middle East and Ukraine.
Military Importance	Swarming can become a European led unprecedented defence capability. Multiple UxVs operating as an intelligent unit will be able to perform disruptive tasks, from monitoring persistently large areas (perform dull, dangerous, dull tasks) to overwhelming adversaries in niche operations, minimizing human risk, mission costs and increasing situational awareness capabilities.

Table 1: Swarming Innovations and Impact

Swarming can make a significant contribution in multiple areas of social and economic interest such as in Unmanned Traffic Management, Autonomous Driving and Urban mobility, all of which utilise swarm technologies. Figure 3 shows that according to forecasts of well-established financial institutions the aggregated market sectors for swarm systems can reach nearly €900 Billion by 2030 with a clear impact in civilian sectors.

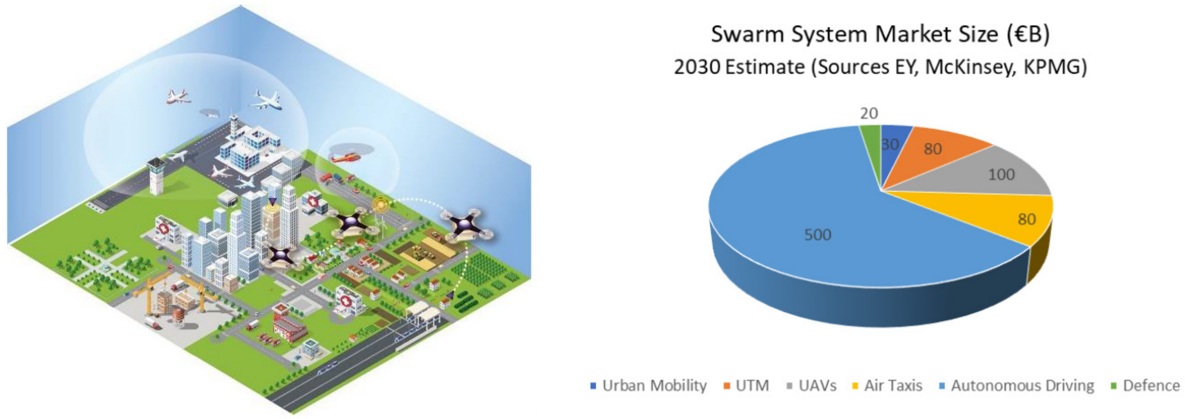


Figure 4: Europe's USpace Unmanned Traffic management[5] (Right) Swarming Market Size[6]

5. CONCLUSIONS

Multiple defence agencies in NATO have announced the intention of adapting swarm technologies to existing weapon systems such as the F-35 fighter/strike jet, the UK Tempest next generation fighter jet and the trilateral (France,

[5] https://www.sesarju.eu/U-space

[6] https://ec.europa.eu/transport/themes/urban/urban_mobility_en and https://www.mckinsey.com/business-functions/sustainability/our-insights/urban-mobility-at-a-tipping-point

Germany, Spain) FCAS aircraft/UAV system. Clearly, swarming technology is being integrated to military capabilities across the world and is beginning to influence defence capabilities. Swarming is a key defence technology which will enable the direct improvement of multiple technological areas such as embedded swarm, AI technologies for automated and autonomous systems, safety, efficiency and effectiveness of cooperative operations of defence systems performed in unstructured, rapidly changing, constrained and contested environments. Swarming, as shown in the Ukraine and Middle East conflict areas, is transforming warfare with the use of swarms of UAVs and loitering ammunitions It is therefore fundamental to develop Autonomous Swarm systems for Europe's defense, security and prosperity and can spin in key technologies to civilian sectors such as transport, robotics and AI.

ACKNOWLEDGEMENTS

Special thanks to the Hellenic MoD, German MoD, EDA, and researchers/staff which have supported all projects mentioned in this paper.

REFERENCES

[1] M. V. K. a. R. P. Myjak, "Unmanned Aerial System (UAS) Swarm Design, Flight Patterns, Communication Type, Applications, and Recommendations," in 2022 IEEE International Conference on Electro Information Technology (eIT), 2022, pp. 586-594.

[2] M. Campion, P. Ranganathan and S. Faruque, "UAV swarm communication and control architectures: a review.," Journal of Unmanned Vehicle Systems, 2018.

[3] T. J. L. S. Chen X, "Review of Unmanned Aerial Vehicle Swarm Communication Architectures and Routing Protocols," Applied Sciences, vol. 10, 2020.

[4] I. Melgar, J. Fombellida, A. Jevtic and J. Seijas, "Swarm architectures for Ground-based Air Defense Systems of Systems," in 7th IEEE International Conference on Industrial Informatics, 2009.

[5] Y. Chen, H. Zhang and M. Xu, "The Coverage Problem in UAV Network: A Survey," in Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Hefei, China, 2014.

[6] E. Galceran and . M. Carreras, "A survey on coverage path planning for robotics," Robotics and Autonomous Systems, vol. 61, no. 12, pp. 1258-1276, 2013.

[7] M. R. Usman, . M. A. Usman, M. A. Yaqub and S. Y. Shin , "UAV Reconnaissance using Bio-Inspired Algorithms: Joint PSO and Penguin Search Optimization Algorithm (PeSOA) Attributes," in 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2019.

[8] D. Luo, S. Li, J. Shao, Y. Xu and Y. Liu, "Pigeon-inspired optimisation-based cooperative target searching for multi-UAV in uncertain environment," International Journal of Bio-Inspired Computation, vol. 19, no. 3, 2022.

[9] N. Nigam, "The Multiple Unmanned Air Vehicle Persistent Surveillance Problem: A Review," Machines, vol. 2, no. 1, pp. 13-72, 2014.

[10] L. Zhou, S. Leng, Q. Liu and Q. Wang, "Intelligent UAV Swarm Cooperation for Multiple Targets Tracking," IEEE Internet of Things Journal, vol. 9, no. 1, pp. 743-754, 2021.

[11] R. Wise and R. Rysdyk, "UAV Coordination for Autonomous Target Tracking," in AIAA Guidance, Navigation, and Control Conference and Exhibit, Keystone, Colorado, 2006.

[12] W. ZHOU, J. LI, Z. LIU and L. SHEN, "Improving multi-target cooperative tracking guidance for UAV swarms using multi-agent reinforcement learning," Chinese Journal of Aeronautics, vol. 35, no. 7, pp. 100-112, 2022.

[13] V. Lappas, H.-S. Shin, A. Tsourdos, D. Lindgren, S. Bertrand, J. Marzat, H. Piet-Lahanier, Y. Daramouskas and V. Kostopoulos, "Autonomous Unmanned Heterogeneous Vehicles for Persistent Monitoring," Drones, 2022.

[14] Lappas, V.; Zoumponos, G.; Kostopoulos, V.; Lee, H.I.; Shin, H.-S.; Tsourdos, A.; Tantardini, M.; Shomko, D.; Munoz, J.; Amoratis, E.; Maragkakis, A.; Machairas, T.; Trifas, A. EuroDRONE, a European Unmanned Traffic Management Testbed for U-Space. Drones 2022, 6, 53. https://doi.org/10.3390/drones6020053

PRESCRIPTIVE AUTO-MAINTENANCE ARCHITECTURE FOR TRUSTWORTHY CROSS-DOMAIN-IMPLEMENTATION IN TECH-DEFENSE

MSc c. Vasiliki Demertzi[1], MSci s. Stavros Demertzis[2]

Abstract

For future defense technologies to increase operational readiness, it is essential to develop innovations that increase equipment dependability, reduce maintenance costs, provide scalability, and improve security and trustworthiness using data and analytics not only to predict when equipment is likely to fail or require maintenance but also to recommend specific maintenance actions to prevent failures or optimize equipment performance. This paper presents an innovative Prescriptive Auto-Maintenance Architecture (PAMA) for dependable cross-domain implementation in defense technology, designed to optimize performance, reduce maintenance costs, and increase overall equipment reliability in response to the abovementioned challenges. The proposed architecture is tailored to the specific requirements of defense technology systems, which require high dependability and trustworthiness. In parallel, it is designed to be implemented across multiple defense technology domains, providing scalable and flexible solutions. In particular, the paper describes the architecture's key components, which include advanced sensors, real-time data analytics, edge and cloud computing, automated maintenance execution, and mechanisms for continuous learning. In addition, architecture is enhanced with innovative techniques such as predictive maintenance with augmented reality, blockchain, and explainable artificial intelligence to improve overall system reliability significantly.

Keywords

Prescriptive Maintenance, Edge Computing, Real-Time Analytics, Explainable Artificial Intelligence, Blockchain.

1. INTRODUCTION

As the complexity and sophistication of defense technology systems continue to increase, so does the need for reliable and efficient maintenance and repair processes, as equipment reliability and availability are parallel to defense mission success. The maintenance and repair of these systems can be challenging and time-consuming, often requiring highly trained and specialized technicians, and can pose significant safety risks if not performed properly. These challenges are further complicated by the need to ensure the trustworthiness and security of the system, especially in the face of increasing cyber threats [1].

In recent years, there has been growing interest in developing advanced auto-maintenance architectures that leverage cutting-edge technologies such as artificial intelligence, blockchain, cloud or edge computing, and augmented reality to optimize the maintenance and repair process and significantly improve the reliability and safety of defense technology systems [2]. Advanced maintenance data-driven strategies are essential to ensure the optimal performance of defense technologies without strict human supervision. For example, collecting data directly from the operational status of equipment, such as signals generated by machine vibrations, audio or thermal imaging signals, or analysis of fluids such as oil, fuel, etc., can be analyzed in real-time to identify the hidden knowledge from this data, thereby providing vital information on the operational status of the equipment, its possible malfunctions, as well as on the vulnerabilities of a portion or all of the equipment [3]. It must be noted that

[1] 1Computer Science Department, School of Science International Hellenic University, Kavala Campus, 65404 Kavala, Greece; vademer@teiemt.grw

[2] 2School of Spatial Planning and Development Faculty of Engineering, Aristotle University of Thessaloniki 54124 Thessaloniki, Greece; demertzs@plandevel.auth.gr

these innovative practices must have interoperability to be applied in cross-domain implementation to provide a comprehensive and integrated solution for the maintenance of various domains of defense technology.

This proposal aims to introduce a PAMA for trustworthy implementation in defense technologies. It is a holistic approach to maintenance that can be applied in various domains of defense technology while also ensuring the trustworthiness and security of the defense ecosystem. This PAMA aims to address the limitations and challenges [4] of current maintenance practices by leveraging cutting-edge technologies such as artificial intelligence, machine learning, and blockchain to enable prescriptive and automated maintenance capabilities in defense technologies.

The rest of the work is structured as follows: initially, the prescriptive maintenance process using real-time data analytics and machine learning is presented, and how this system enables defense organizations to make informed decisions based on the provided insights the system provides. Then, the third chapter presents how remote monitoring and diagnosis systems of the proposed PAMA can provide maintenance teams with a more comprehensive view of equipment performance, allowing them to identify trends and patterns that may not be visible with manual monitoring alone. The cybersecurity considerations methodology is presented in the next chapter, which explains how the proposed architecture, by incorporating several novel security measures, can provide a secure and reliable platform for maintenance operations in defense technology systems. Chapter six presents the structured and comprehensive implementation plan and how the architecture can be successfully integrated with the existing maintenance practices in the defense technology. Finally, in the concluding chapter, there is a discussion of the proposed methodology and how future research to be followed

2. OVERVIEW OF THE PROPOSED PAMA

Prescriptive maintenance is a proactive maintenance strategy that uses real-time data analytics and machine learning to forecast and recommend maintenance actions before a failure occurs [5]. Auto-maintenance architecture is a critical strategy that helps ensure equipment operates optimally, ensuring its safety, reliability, and longevity without strict human observation and supervision [6]. Combining the above strategies can produce a novel architecture for the next generation of defense technologies that involves rethinking how components are organized, introducing new maintenance techniques, or optimizing specific tasks. This work provides a PAMA for reliable cross-domain implementation in defense technology, which is intended to maximize performance, minimize maintenance costs, and boost overall equipment reliability, combining the above strategies. The proposed architecture is adapted to the special needs of defense technology systems, which necessitate great reliability and credibility. The PAMA proposed in this paper consists of four key layers: the infrastructures layer, the intelligence layer, the maintenance layer, and the security and privacy layer. Each layer plays a critical role in the maintenance process and contributes to the effectiveness and efficiency of the overall architecture. The following diagram depicts the PAMA architecture.

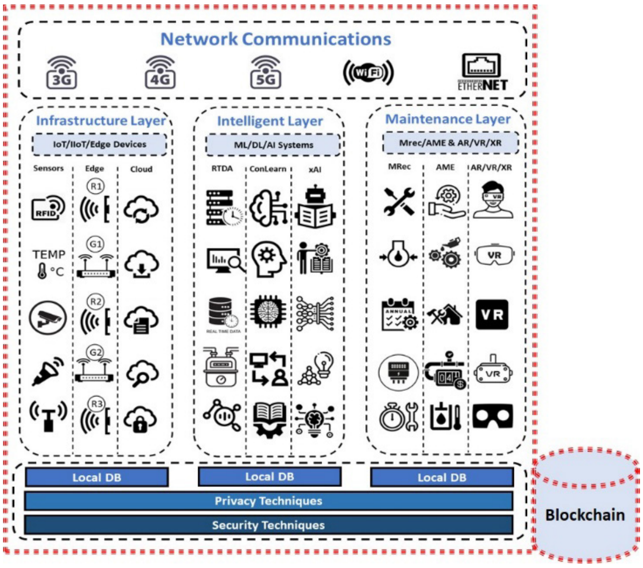


Figure 1. Prescriptive Auto-Maintenance Architecture diagram

In this diagram, the infrastructures layer collects data from various sources within the defense technology system and transmits it to the local or centralized (cloud) database. The intelligence layer processes and analyzes the data to identify patterns and trends that inform the prescriptive maintenance component. The maintenance layer recommends maintenance actions or automatically implements some of them. Also, it provides the ability to produce replacement parts and components quickly and cost-effectively using 3D printing technology. The security and privacy layer applies security policies, privacy methods, and encryption techniques to the architecture, ensuring that the system is secure and privacy-preserving. In addition, using blockchain technology, the PAMA enables secure data sharing between stakeholders in the maintenance process.

It must be noted that cross-domain implementation of the PAMA refers to the application of the proposed technology solution to various domains of defense technology, such as software, hardware, and networking. In many defense technology systems, maintenance is handled separately for each domain, leading to a need for coordination and integration between different maintenance activities. This can result in inefficiencies, duplication of effort, and an increased risk of errors and system failures. By implementing a prescriptive auto-maintenance architecture that covers various domains of defense technology, cross-domain implementation can address these challenges and provide a more holistic and integrated approach to maintenance.

The proposed architecture addresses the maintenance needs of various domains of defense technology, including software, hardware, and networking [7]. For example, the architecture can monitor and analyze software code to identify potential issues, such as bugs or security vulnerabilities. The architecture can also monitor and analyze hardware performance data to identify issues with components or subsystems. The architecture can also monitor and analyze network traffic to identify potential issues with connectivity or security.

By addressing the maintenance needs of various domains of defense technology, the proposed architecture can provide a more comprehensive and integrated approach to maintenance. The architecture can provide insights and recommendations for maintenance across different domains, allowing maintenance teams to coordinate and prioritize their activities more effectively. Also, it can improve maintenance efficiency and effectiveness, reducing the risk of system failures and downtime.

3. PRESCRIPTIVE MAINTENANCE

Prescriptive maintenance is a key feature of the proposed PAMA, which aims to leverage data analytics and machine learning to monitor equipment performance and predict when maintenance will be needed. This approach enables maintenance teams to be proactive in their approach to maintenance, addressing issues before they become critical and reducing the risk of system failures and downtime. Prescriptive maintenance involves collecting and analyzing data from various sources, such as sensors, logs, and other data sources from the infrastructure layer. Specifically, Defense organizations can collect accurate and reliable data about their equipment's condition and performance by using the advanced sensor architecture of the infrastructure layer that includes sensor types, placement, health monitoring, and data transmission. In addition, the data can be collected from edge devices. PAMA incorporates edge computing that enables data processing, storage, and analysis at the network's edge, closer to the sensors or devices that generate the data, such as routers, switches, gateways, sensors, cameras, and other IoT/IIoT devices, as well as edge servers. The edge computing application management tools can monitor and control edge workloads to ensure that edge devices run optimally and meet the required performance criteria. Finally, the data collection can be done by cloud-based infrastructures that provide scalability, cost savings, flexibility, reliability, and security [8].

Then the data is processed and analyzed using advanced machine-learning algorithms and statistical models to identify patterns and trends that may indicate potential issues with the equipment. The intelligent layer achieves this. Specifically, the intelligent layer includes the real-time data analytics system [9]. This is implemented to process data collected by data repositories or producers. It involves several components that work together to process, analyze, and visualize data in real time. The first step is collecting data from PAMA sources, such as device logs, data feeds, etc. The data processing sub-system is responsible for cleansing and transforming data into a format that can be analyzed. The data storage sub-system stores the transformed data, and real-time analytics is used for insights into the data, enabling organizations to make informed decisions based on the real conditions provided by the system. This component uses extensive machine learning algorithms, statistical analysis, or other analytical techniques to detect anomalies, identify trends, and provide insights into the data. Data validation, data visualization, alerting and notifications, data governance and security, optimization, and improvement, and swarm intelligence strategies are all key components [10].

In addition, the intelligent layer includes the continuous learning sub-system. The specific sub-system's architecture is designed to learn and adapt continuously over time, incorporating new data and feedback to improve predictive accuracy and make more accurate maintenance recommendations. It includes model training, model deployment, continuous evaluation, feedback loop, and feedback from maintenance technicians and other stakeholders. This allows the system to learn and improve its maintenance forecasts and recommendations to improve overall equipment performance and reliability [11].

To thoroughly upgrade the maintenance environment, the PAMA includes an explainable AI (xAI) sub-system in the intelligent layer. The xAI is used to improve the system's transparency and interpretability, enabling maintenance technicians and other stakeholders to understand better how the system arrives at its maintenance recommendations. It is also used to validate the accuracy and effectiveness of the machine learning models, identify the strengths and weaknesses of the models, evaluate their performance under different conditions, and verify that they are not making biased or unfair recommendations. Additionally, xAI improves the user interface of the PAMA, enabling stakeholders to understand the system's recommendations better and provide more intuitive and user-friendly feedback. This helps to improve trust in the system, reduce downtime, and increase equipment reliability [12].

The data analysis insights inform the architecture's Maintenance Layer, which then recommends maintenance actions. The system can predict when maintenance will be required and what actions should be taken to address potential issues. For example, it may recommend replacing a specific component or performing a specific maintenance activity based on the data analysis. Specifically, this layer includes three novel implementations that significantly upgrade the traditional maintenance process.

Firstly, the Maintenance Recommendations sub-system recommends the appropriate actions based on the equipment's condition and performance, including the recommended maintenance action, parts needed, and estimated time required. The architecture is designed to provide accurate, specific, and timely recommendations to help organizations optimize their equipment performance, reduce maintenance costs, and improve overall equipment reliability. It includes the Maintenance Recommendation Engine, Maintenance Action Planning, Additive Manufacturing, and User Interface. A key component of this sub-system is additive manufacturing which provides the ability to produce replacement parts and components quickly and cost-effectively using 3D printing technology, reducing the need for complex supply chains and inventory management. This is achieved by creating digital models of the parts and feeding them into a 3D printer. The 3D printer then creates the parts layer by layer, using materials such as plastics, metals, or composites.

Secondly, the Automated Maintenance Execution system provides a highly efficient and effective next-generation maintenance process. It consists of three key components: Maintenance Execution Engine, Workflow Management, and Integration with Asset Management System. The Maintenance Execution Engine is responsible for automatically executing some maintenance actions recommended by the data analytics and machine learning system. At the same time, the Workflow Management component is responsible for managing the overall maintenance process in order to help organizations optimize equipment performance, reduce maintenance costs, and increase equipment reliability.

Thirdly, the Maintenance with Augmented Reality (MAR) sub-system aims to help technicians perform maintenance and repair tasks more efficiently and accurately by providing real-time guidance and feedback using augmented reality technology. The key components of the MAR system include maintenance task identification, MAR visualization, procedural guidance, and quality assurance. The MAR system can help improve efficiency, reduce downtime, and increase equipment reliability by providing clear and intuitive instructions and a standardized and consistent maintenance approach based on best practices and industry standards [13].

In summary, predictive maintenance is a critical feature of the proposed PAMA, which aims to leverage data analytics and machine learning to monitor the performance of equipment and predict when maintenance will be needed. This approach enables teams to be proactive in their approach to maintenance, reducing the risk of system failures and downtime and improving the efficiency and effectiveness of maintenance operations.

4. REMOTE MONITORING AND DIAGNOSIS

Remote monitoring and diagnosis are critical features of the proposed prescriptive auto-maintenance architecture. It leverages sensors, edge computing, and IoT/IIoT devices to monitor equipment performance and detect issues in real-time, allowing maintenance teams to address potential problems quickly. The architecture includes advanced sensors that can collect a wide range of data about the equipment. These include temperature, pressure, vibration, humidity, and other sophisticated sensors relevant to the equipment's function and defense industry environment. The sensors are placed strategically to collect relevant data about the equipment's condition and performance. This is critical to ensure accurate data collection and to minimize interference from other equipment or external factors. Also, the proposed advanced sensor architecture includes health monitoring capabilities to ensure that the sensors function correctly. This involves monitoring sensor drift and calibration processes in order to identify any failures or issues [14].

In addition, the proposed architecture includes advanced application management in order to monitor whether devices are working effectively. For example, the proposed application management tools can monitor and control devices' workloads, ensuring they run optimally and meet the required performance criteria. Also, the PAMA architecture uses consolidated dashboards and visualizations from several sub-systems like edge computing, cloud infrastructure, xAI sub-system, etc., that allow users to easily monitor the equipment's performance, identify issues, understand the system's recommendations better, and provide more intuitive feedback about maintenance and repair.

Moreover, the alerting and notifications component notifies users when specific events or conditions are met. This component uses email, SMS, or other messaging technologies to alert users of critical events in real-time. Finally, the feedback loop component incorporates feedback from maintenance technicians and other stakeholders. This feedback can be used to improve the accuracy of the machine learning models, refine the maintenance recommendations, and identify areas for improvement. Also, enabling stakeholders to provide feedback on the maintenance recommendations, helps identify areas where the PAMA needs improvement, providing a continuous adaptive cycle for the system.

The benefits of remote monitoring and diagnosis are significant. It enables maintenance teams to monitor equipment performance and detect real-time issues, reducing the risk of system failures and downtime. By addressing potential issues before they become critical, maintenance teams can be more proactive in their approach to maintenance. This can also result in cost savings by reducing the need for reactive and costly maintenance practices.

In addition, remote monitoring and diagnosis can provide maintenance teams with a more comprehensive view of equipment performance, allowing them to identify trends and patterns that may not be visible with manual monitoring alone. This can help maintenance teams to improve the efficiency and effectiveness of maintenance operations and reduce the risk of errors.

5. CYBERSECURITY CONSIDERATIONS

Cybersecurity is a critical consideration in the proposed PAMA architecture [15]. Given the sensitive nature of defense technology systems, it is important to ensure that the architecture is designed to prevent cyber-attacks and protect data security and privacy. To address cybersecurity considerations, the proposed architecture includes several features and controls designed to ensure data security and prevent cyber-attacks. These features and controls include [16]:

1. Access controls: Access controls are used to limit access to the system to authorized personnel only. This includes authentication and authorization mechanisms to ensure that only authorized users can access the system and data, and techniques such as role-based access controls, where access is restricted based on the

user's role or level of authorization.

2. Encryption: Data encryption ensures that data transmitted over the network is secure and cannot be intercepted by unauthorized users. Encryption can also protect sensitive data at rest, ensuring that unauthorized users cannot access it.
3. Secure data storage and sharing: Sensitive data is stored in secure, encrypted storage locations to protect it from theft or tampering. The system implements regular backups and redundancy to ensure that the data is not lost in the event of a hardware failure or other issues. If data needs to be shared with third parties, the privacy sub-system incorporates techniques such as secure data-sharing protocols and differential privacy to ensure that the data is transmitted securely and only to authorized parties.
4. Blockchain: The maintenance with a blockchain system enables secure data sharing between different stakeholders in the maintenance process, providing a secure, transparent, and immutable record of equipment performance, maintenance actions, and other relevant data. The system's key components include blockchain record creation, verification, and storage. Authorized parties, such as maintenance technicians, equipment owners, or defense authorities, can access the blockchain record to view the maintenance history. This improves the security and transparency of defense maintenance records and provides a tamper-proof and decentralized record of all activities performed [17].
5. Monitoring and logging: The system includes monitoring and logging capabilities designed to detect and record any suspicious or unauthorized activity. This involves the use of intrusion detection and prevention systems, network monitoring tools, and security information and event management (SIEM) solutions to identify and respond to security threats. This enables the system to identify potential cyber-attacks and respond quickly to prevent damage or data loss.
6. Vulnerability assessments: Regular vulnerability assessments are conducted to identify and address any security vulnerabilities in the system. This includes regular penetration testing to identify any weaknesses in the system that cyber-attackers could exploit.
7. Compliance and auditing: To ensure compliance with relevant regulations and policies related to data privacy and security, the system also incorporates auditing and monitoring capabilities.
8. Disaster recovery and business continuity: The system includes disaster recovery, and business continuity plans to ensure that the system can recover quickly in the event of a cyber-attack or other disruption.

The proposed PAMA architecture includes multiple features and controls designed to ensure data security, and privacy and prevent cyber-attacks. By incorporating these security measures, the architecture provides a secure and reliable platform for maintenance operations in defense technology systems.

6. IMPLEMENTATION PLAN

The implementation plan for the proposed PAMA architecture may vary depending on the specific needs and requirements of the defense technology system. The specific stages of the implementation plan for the proposed architecture are the following:

1. Planning and analysis: The first stage of the implementation plan involves planning and analysis. This involves thoroughly assessing the existing maintenance practices used in the defense technology system and identifying the areas needing improvement. This stage also involves setting goals and objectives for implementing the proposed architecture.
2. System design and development: The second stage of the implementation plan involves system design and development. This involves designing and developing the prescriptive auto-maintenance architecture, including the various components and their integration with the existing maintenance practices. This stage also involves selecting the appropriate technologies, tools, and platforms to implement the architecture.
3. Testing and validation: The third stage of the implementation plan involves testing and validation. This involves testing the prescriptive auto-maintenance architecture to ensure that it meets the goals and objectives set in the planning and analysis stage. This stage also involves validating the architecture's performance and accura-

cy in predicting maintenance needs.

4. Deployment and integration: The fourth stage of the implementation plan involves deploying and integrating the prescriptive auto-maintenance architecture with the existing maintenance practices. This involves ensuring that the architecture is compatible with the existing systems and integrates seamlessly with the existing maintenance workflows. This stage also involves training maintenance personnel on using the new architecture and its various components.
5. Monitoring and evaluation: The final stage of the implementation plan involves monitoring and evaluation. This involves monitoring the performance of the prescriptive auto-maintenance architecture to ensure that it meets the goals and objectives set in the planning and analysis stage. This stage also involves evaluating the architecture's impact on the overall maintenance process and identifying areas for further improvement.

It is important to note that the implementation plan is flexible and adaptable to the changing needs and requirements of the defense technology system. Also, it includes a contingency plan in case of unforeseen issues or challenges. In terms of deploying and integrating the architecture with existing maintenance practices, the following steps will be taken:

1. Identify existing maintenance workflows and processes: This involves understanding how maintenance is performed within the defense technology system and identifying workflows and processes that need to be integrated with the prescriptive auto-maintenance architecture.
2. Identify integration points: This involves identifying the points of integration between the prescriptive auto-maintenance architecture and the existing maintenance workflows and processes. This may involve integrating existing software applications, databases, or other systems.
3. Develop integration plan: Based on the identified integration points, a plan should be developed to integrate the prescriptive auto-maintenance architecture with the existing maintenance workflows and processes. This may involve developing custom integrations or using third-party integration tools.
4. Training maintenance personnel: Training should be provided to maintenance personnel using the prescriptive auto-maintenance architecture and its various components. This may include training in data analysis and machine learning algorithms.
5. Monitor and evaluate: The performance of the prescriptive auto-maintenance architecture should be monitored and evaluated to ensure that it meets the goals and objectives set in the planning and analysis stage. This may involve identifying areas for improvement and making changes to the implementation plan as needed.

The implementation plan for the proposed PAMA architecture involves several stages, including planning and analysis, system design and development, testing and validation, deployment and integration, and monitoring and evaluation. By following a structured and comprehensive implementation plan, the architecture can be successfully integrated with the existing maintenance practices in the defense technology system, improving overall maintenance efficiency and effectiveness.

7. CONCLUSIONS

An innovative PAMA architecture can help organizations optimize equipment performance, reduce maintenance costs, and increase equipment reliability. The proposed architecture is designed to provide a more efficient and effective approach to maintenance in defense technology systems. By leveraging data analytics, machine learning, and IoT technologies, the architecture provides a proactive and predictive approach to maintenance, enabling maintenance teams to address potential issues before they become critical.

The key components of the proposed architecture include prescriptive maintenance using extensive adaptive AI methodologies, remote monitoring and diagnosis, additive manufacturing, automated maintenance execution, and maintenance with augmented reality. These components work together to provide a comprehensive and integrated approach to maintenance, reducing downtime, improving efficiency, and reducing costs. In addition, the security and privacy layer use advanced security, privacy, encryption techniques, and blockchain to ensure that authorized parties only access sensitive data with the appropriate credentials and that relevant policies and regulations use it.

The implementation plan for the proposed architecture involves several stages, including planning and analysis, system design and development, testing and validation, deployment and integration, and monitoring and evaluation. Following a structured and comprehensive implementation plan, the proposed architecture can be successfully integrated with existing maintenance practices in defense technology systems.

The benefits of the proposed architecture are numerous. Specifically, it enables maintenance teams to be more proactive in their approach to maintenance, reducing the risk of system failures and downtime. It can also result in significant cost savings and increased efficiency. By incorporating cybersecurity measures, the architecture can ensure data security and prevent cyber-attacks in the defense industry.

In areas for further research and development, there is potential to improve the performance and accuracy of the machine learning algorithms used in the predictive maintenance component of the architecture. There is also potential to further optimize IoT devices and sensors for remote monitoring and diagnosis.

REFERENCES

[1] A. Bousdekis, D. Apostolou, and G. Mentzas, "Predictive Maintenance in the 4th Industrial Revolution: Benefits, Business Opportunities, and Managerial Implications," IEEE Eng. Manag. Rev., vol. 48, no. 1, pp. 57–62, 2020, doi: 10.1109/EMR.2019.2958037.

[2] D. S. Jasi, R. O. Bura, and Jupriyanto, "Innovation of Defense Technology Audit to Support Self-Reliant National Defense Industry," in 2019 IEEE 6th Asian Conference on Defence Technology (ACDT), Aug. 2019, pp. 32–38. doi: 10.1109/ACDT47198.2019.9072944.

[3] S. L. Mak, W. F. Tang, C. H. Li, and C. C. Lee, "A Critical Review on Smart Maintenance Decision Support System based on IIoT technology," in 2022 IEEE International Conference on Industrial Technology (ICIT), Dec. 2022, pp. 1–5. doi: 10.1109/ICIT48603.2022.10002806.

[4] S. T. Yimer, Y. S. Molla, and E. Alemneh, "Predicting Software Maintenance Type, Change Impact, and Maintenance Time Using Machine Learning Algorithms," in 2022 International Conference on Information and Communication Technology for Development for Africa (ICT4DA), Aug. 2022, pp. 37–41. doi: 10.1109/ICT4DA56482.2022.9971350.

[5] A. Consilvio et al., "Prescriptive Maintenance of Railway Infrastructure: From Data Analytics to Decision Support," in 2019 6th International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), Jun. 2019, pp. 1–10. doi: 10.1109/MTITS.2019.8883331.

[6] Z. Zhiwei, S. Haosong, G. Dongying, H. Fangfang, L. Qinghai, and C. Chuanjian, "IT Automatic Operation and Maintenance Service System Based on SaaS Architecture," in 2022 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS), Sep. 2022, pp. 662–665. doi: 10.1109/TOCS56154.2022.10015925.

[7] "International Standard-Software Interface for Maintenance Information Collection and Analysis (SIMICA)," IECIEEE 616362021, pp. 1–52, Jun. 2021, doi: 10.1109/IEEESTD.2021.9451889.

[8] S. Choubey, R. Benton, and T. Johnsten, "Prescriptive Equipment Maintenance: A Framework," in 2019 IEEE International Conference on Big Data (Big Data), Sep. 2019, pp. 4366–4374. doi: 10.1109/BigData47090.2019.9006213.

[9] A. Batyuk, V. Voityshyn, and V. Verhun, "Software Architecture Design of the Real- Time Processes Monitoring Platform," in 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), Dec. 2018, pp. 98–101. doi: 10.1109/DSMP.2018.8478589.

[10] J. MATTIOLI, P. PERICO, and P.-O. ROBIC, "Improve Total Production Maintenance with Artificial Intelligence," in 2020 Third International Conference on Artificial Intelligence for Industries (AI4I), Sep. 2020, pp. 56–59. doi: 10.1109/AI4I49448.2020.00019.

[11] W. Cui, Z. Xue, and K.-P. Thai, "Performance Comparison of an AI-Based Adaptive Learning System in China," in 2018 Chinese Automation Congress (CAC), Aug. 2018, pp. 3170–3175. doi: 10.1109/CAC.2018.8623327.

[12] C. K. Tantithamthavorn and J. Jiarpakdee, "Explainable AI for Software Engineering," in 2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE), Aug. 2021, pp. 1–2. doi: 10.1109/ASE51524.2021.9678580.

[13] R. Buettner, J. Breitenbach, K. Wannenwetsch, I. Ostermann, and R. Priel, "A Systematic Literature Review of Virtual and Augmented Reality Applications for Maintenance in Manufacturing," in 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), Jun. 2022, pp. 545–552. doi: 10.1109/COMPSAC54236.2022.00099.

[14] S. D. Milić and B. M. Babić, "Toward the Future—Upgrading Existing Remote Monitoring Concepts to IIoT Concepts," IEEE Internet Things J., vol. 7, no. 12, pp. 11693–11700, Sep. 2020, doi: 10.1109/JIOT.2020.2999196.

[15] L. Trotter, M. Harding, M. Mikusz, and N. Davies, "IoT-Enabled Highway Maintenance: Understanding Emerging Cybersecurity Threats," IEEE Pervasive Comput., vol. 17, no. 3, pp. 23–34, Apr. 2018, doi: 10.1109/MPRV.2018.03367732.

[16] A. Mohammed and G. George, "Vulnerabilities and Strategies of Cybersecurity in Smart Grid - Evaluation and Review," in 2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE), Mar. 2022, pp. 1–6. doi: 10.1109/SGRE53517.2022.9774038.

[17] W. Lang Jensen, S. Jessing, W.-Y. Chiu, and W. Meng, "AirChain - Towards Blockchain-based Aircraft Maintenance Record System," in 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Feb. 2022, pp. 1–3. doi: 10.1109/ICBC54727.2022.9805550.

Authors

MSc c. Vasiliki Demertzi

Vasiliki Demertzi is a highly motivated MSc candidate in Computer Science at the International Hellenic University, Kavala Campus, with a passion for software development and emerging technologies. Vasiliki completed her BSc in Computer Science at the same institution, where she honed her skills in programming languages such as Python, Java, and C++. She has hands-on experience in machine learning, web development, and database systems. Vasiliki has completed several notable projects during her academic journey, including an education game to learn software development, a network traffic analysis model for cyber security, and an adversarial machine learning defense system. In the summer of 2022, Vasiliki interned as a validator of "Root CA Operator" in Greece at the Aristotle University of Thessaloniki, where now working on a regular base. Vasiliki is fluent in Greek and English and has an intermediate command of German. She holds certifications such as the Certified Cyber Intelligence Specialist and the Internet & Cybersecurity on Windows and Social Media. Her dedication to her research has led her to publish several research articles in scientific journals (https://scholar.google.gr/citations?user=NTN4ywoAAAAJ&hl).

MSci s. Stavros Demertzis

MSci Stavros Demertzis is an integrated master's student in the final year at the School of Spatial Planning and Development, Faculty of Engineering, Aristotle University of Thessaloniki, Greece. With a strong background in machine learning, automation, electrical sustainable energy systems, and operations and maintenance practices in environmental applications, Stavros has dedicated his career to advancing the understanding and application of innovative, next-generation techniques in real-world contexts. MSci Stavros Demertzis, after completing his studies for an integrated master's degree, will pursue his doctoral degree, focusing on sustainable environmental and mechanical architectures and their impact on smart cities. Stavros is fluent in Greek and English and has an intermediate command of German. He has published multiple research articles in scholarly journals (https://scholar.google.gr/citations?user=VglPkFsAAAAJ&hl).

REVOLUTIONISING CBRN DEFENCE THROUGH NANOTECHNOLOGY-BASED ENCAPSULATION OF CONDUCTING COPOLYMERS WITHIN PAMAM DENDRIMERS

Elçin Tören[1, 2]

Abstract

This project aims to develop advanced nanocomposite materials for Chemical, Biological, Radiological, and Nuclear (CBRN) defence applications by encapsulating conducting copolymers of polyaniline, polythiophene, and polyacetylene within polyamidoamine (PAMAM) dendrimers. The in-situ copolymerisation technique offers an efficient method for encapsulation, resulting in uniform distribution and enhanced stability, processability, and functionality of the conducting copolymers. These encapsulated copolymer nanocomposites have the potential to be utilised in a wide range of CBRN defence applications, including sensing, protective equipment, gas filtration, and decontamination. The successful completion of this project is expected to contribute significantly to the development of novel materials and solutions for CBRN defence, revolutionising the industry and offering improved protection and detection capabilities.

Keywords

Nanocomposite materials, Chemical, Biological, Radiological, and Nuclear (CBRN) defence, Protective equipment.

1. AIMS AND OBJECTIVES OF THE PROJECT

CBRN threats have a long history, with chemical warfare agents being used as early as World War I. These threats have since evolved, resulting in the development of many toxic gaseous molecules. Additionally, toxic biological species, such as bacteria and viruses, have also been used for war purposes. However, the development, research, and storage of biological and chemical weapons were banned by the Biological Weapons Convention in 1972 and the Chemical Weapons Convention in 1997 [1]. Nanotechnology has the potential to revolutionise the defence industry by enabling the development of highly efficient and selective CBRN decontamination systems, utilising nanomaterials like nanoparticles, nanotubes, and nanofibers that can interact with CBRN agents at the molecular level for enhanced detection, neutralisation, and removal capabilities [2].

Nanofibers have shown great potential in the field of CBRN defence due to their unique properties, such as high surface area-to-volume ratio, high porosity, and small pore size [3]. The properties of nanofibers make them highly effective for filtration, separation, and personal protective equipment applications, efficiently filtering out a wide range of airborne particulates, including biological and chemical agents in CBRN defence.[4].This is particularly important for soldiers and first responders who may need to wear protective clothing for extended periods of time in hot and humid environments. Nanofiber-based fabrics can also be designed to provide protection against both biological and chemical agents, making them highly versatile for use in a range of CBRN defence applications. Furthermore, the high porosity and small pore size of nanofibers make them ideal for use in decontamination applications [5]. One significant advantage of using PAMAM dendrimers to encapsulate conducting copolymers is their improved stability. The encapsulation process protects the copolymers from degradation and other environmental factors, enhancing their overall lifespan and functionality [6]. Additionally, the dendrimers can provide a controlled environment for the copolymers, allowing for the attachment of specific recognition elements,

[1] Respilon Membranes-Research and Development Centre, Prague, Czech Republic

[2] Technical University of Liberec-Textile Engineering, Liberec, Czech Republic elcin.toren@tul.cz

such as antibodies or aptamers, to the copolymer surface. This can significantly enhance the sensitivity and selectivity of the resulting materials for detecting chemical and biological warfare agents [7]. Another advantage of the encapsulation process is the potential to incorporate catalytic or reactive functionalities within the dendrimer structure. This can enable the development of advanced protective coatings and decontamination materials with enhanced capabilities for neutralising CBRN agents [8].

This project aims to develop advanced materials for CBRN defence by copolymerising conducting polymers (polyaniline, polythiophene, and polyacetylene) and encapsulating them within PAMAM dendrimers. This combination has the potential to create materials with tailored properties for improved sensing, adsorption, and protection in various CBRN-related projects. The polyamidoamine encapsulation of polyaniline, polyacetylene, and polythiophene copolymers by nanotechnology methods can be applied to various CBRN defence applications, including sensing, protective coatings, decontamination, gas filtration, and personal protective equipment (PPE). Sensing is one of the most significant applications of these encapsulated conducting polymers. The PAMAM dendrimers provide a protective environment for the conducting polymers, enhancing their sensitivity and selectivity for detecting chemical and biological warfare agents. The addition of specific recognition elements, such as antibodies or aptamers, to their surface, further improves the sensing capabilities of the material. Another application is the development of advanced protective coatings for equipment and infrastructure. The encapsulated conducting polymer copolymers can be designed with catalytic or reactive functionalities incorporated within the dendrimer structure, providing a barrier against CBRN agents and facilitating their neutralisation [9].

PAMAM dendrimers encapsulating conducting polymer copolymers can also be used to create materials that can adsorb, neutralise, or degrade CBRN agents, making them suitable for use in decontamination systems [10]. The dendrimers can be designed with reactive or catalytic groups that facilitate the decontamination and neutralisation of CBRN agents. Encapsulated conducting polymer copolymers within PAMAM dendrimers can also be employed to develop novel gas filtration materials with improved adsorption and selectivity properties. These materials can effectively remove harmful gases, such as chemical warfare agents or toxic industrial chemicals, from the environment, providing protection for personnel and infrastructure [8].

In summary, the copolymerisation of polyaniline, polythiophene, and polyacetylene, combined with the encapsulation within PAMAM dendrimers, presents a promising avenue for the development of advanced materials for CBRN applications. This approach can enhance the stability, processability, and functionality of the conducting polymers, enabling their use in various CBRN-related applications, such as sensing, protective equipment, and decontamination.

1.1. SPECIFIC OBJECTIVES OF THE PROJECT

The EU defence industry is increasingly focused on developing advanced materials and technologies to counter CBRN threats. This project aims to synthesise and encapsulate conducting polymers within PAMAM dendrimers for improved stability, processability, and functionality in various CBRN defence applications. By addressing critical aspects such as sensing, protective coatings, gas filtration, and personal protective equipment, this project contributes to the EU defence industry's efforts to safeguard its citizens and infrastructure from potential CBRN incidents.

The development and application of nanotechnology-based materials, particularly copolymers of polyaniline, polythiophene, and polyacetylene encapsulated within PAMAM dendrimers, is a novel aspect of this project. These materials have the potential to enhance the performance of CBRN defence systems and open up new avenues for research and innovation. The success of this project could lead to significant advancements in CBRN defence technology, potentially saving lives and protecting critical infrastructure. The breakthrough use of nanotechnology in this project highlights the importance of continued research and innovation in the field of CBRN defence, making it of significant interest to both the scientific community and the general public.

The specific objectives for this project include the following:

1. Synthesis and characterisation of copolymers of polyaniline, polythiophene, and polyacetylene with tailored

properties for CBRN defence applications.

2. Development of a method for encapsulating the synthesised copolymers within polyamidoamine (PAMAM) dendrimers to enhance their stability, processability, and functionality.
3. Design and fabrication of highly sensitive and selective sensors for the detection of chemical and biological warfare agents using the synthesised copolymers and PAMAM dendrimers.
4. Creation of advanced protective coatings for equipment and infrastructure that can provide a barrier against CBRN agents and facilitate their neutralisation.
5. Development of novel gas filtration materials with improved adsorption and selectivity properties for the removal of harmful gases and chemical agents from the environment.
6. Synthesis of lightweight, flexible, and highly protective materials for use in personal protective equipment, such as suits, gloves, and masks.
7. Evaluation of the effectiveness of the developed materials in real-world CBRN defense applications and comparison with existing technologies.

1.2. WORK PACKAGES

The following work package table provides an overview of the key stages of the project and their respective tasks. This table serves as a roadmap for the project, helping to allocate resources, track progress, and ensure that all tasks are completed in a timely and efficient manner.

Table 1. Work packages of the project.

Work Package (WP)	**Description**	**Tasks**
WP1	Material Synthesis	1. Synthesise copolymers 2. Optimise synthesis process
WP2	Dendrimer Encapsulation	1. Develop encapsulation method 2. Optimise encapsulation process
WP3	Material Characterisation	1. Perform analytical characterisations 2. Analyse and interpret results
WP4	Prototype Development	1. Design and fabricate prototypes 2. Optimise performance and integration
WP5	Testing and Evaluation	1. Conduct laboratory and field tests 2. Compare results with existing technologies
WP6	Optimisation	1. Optimise material properties and prototypes 2. Validate optimised materials and prototypes
WP7	Documentation and Dissemination	1. Document research findings 2. Publish results in journals and conferences

3. MATERIALS AND METHODS

3.1. MATERIALS

The materials used in this project will include aniline, thiophene, and acetylene monomers, ammonium persulfate (APS) oxidant, polyamidoamine (PAMAM) dendrimers, suitable solvents (such as water or ethanol), and suitable acid (such as hydrochloric acid (HCl)).

3.2. METHODS

Polyamidoamine encapsulation of polyaniline, polythiophene and polyacetylene copolymers was achieved by using nanotechnology methods. In situ copolymerisation is carried out by adding aniline, thiophene and acetylene monomers to a PAMAM dendrimer solution under continuous stirring. The pH of the mixture should be adjusted to an acidic range using hydrochloric acid and oxidant (APS) added to initiate the polymerisation reaction. The reaction mixture should be stirred for a period of time to complete the copolymerisation and allow the copolymer to be encapsulated in PAMAM dendrimers. Figure 1 illustrates the step-by-step process for encapsulating the conducting copolymers within PAMAM dendrimers using nanotechnology methods. The resulting encapsulated copolymer is purified by centrifugation or filtration and washed with a suitable solvent to remove any remaining reactants or by-products. Finally, the encapsulated copolymer is dried under a vacuum or in a controlled environment to remove residual solvent. The successful encapsulation of copolymers in PAMAM dendrimers was confirmed by various analytical techniques such as FTIR, XRD, SEM and TEM. These nanocomposite materials can be used for various CBRN defence applications, including sensors, protective coatings, gas filtration materials and personal protective equipment.

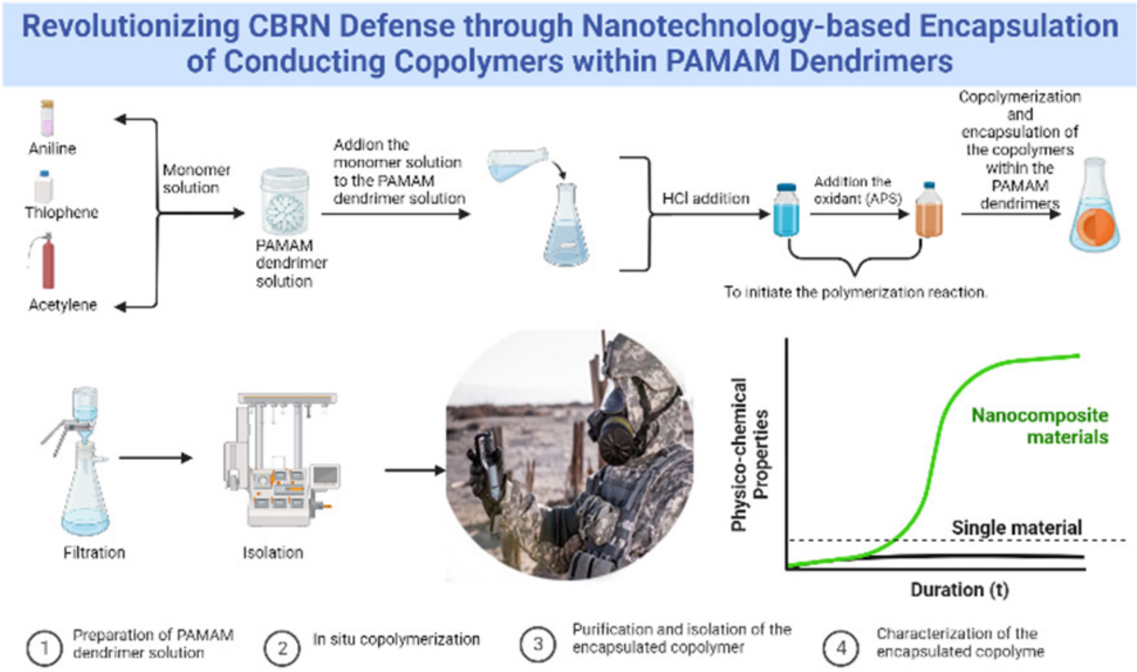

Revolutionizing CBRN Defense through Nanotechnology-based Encapsulation of Conducting Copolymers within PAMAM Dendrimers
Aniline
Thiophene
Acetylene
Monomer solution
PAMAM dendrimer solution
Addion the monomer solution to the PAMAM dendrimer solution
HCl addition
Addition the oxidant (APS)
Copolymerization and encapsulation of the copolymers within the PAMAM dendrimers
To initiate the polymerization reaction.
Filtration
Isolation
Physico-chemical Properties
Nanocomposite materials
Single material
Duration (t)
1 Preparation of PAMAM dendrimer solution
2 In situ copolymerization
3 Purification and isolation of the encapsulated copolymer
4 Characterization of the encapsulated copolyme

Figure 1. Schematic representation of the nanotechnology-based encapsulation process of polyaniline, polythiophene, and polyacetylene copolymers within PAMAM dendrimers.

4. CONCLUSIONS

This project aims to develop novel nanocomposite materials by encapsulating polyaniline, polythiophene, and polyacetylene copolymers within polyamidoamine (PAMAM) dendrimers. The in-situ polymerisation method allows for efficient encapsulation and uniform distribution of the conducting copolymers within the PAMAM dendrimer structure. By optimising the reaction conditions, including monomer concentrations, dendrimer-to-monomer ratio, reaction time, and pH, high-quality encapsulated copolymer nanocomposites can be obtained. These materials have the potential to be used in a variety of Chemical, Biological, Radiological, and Nuclear (CBRN) defence applications, including sensing, protective equipment, and decontamination.

The successful completion of this project is expected to yield several significant results that could potentially revolutionise the field of Chemical, Biological, Radiological, and Nuclear (CBRN) defence. One of the expected outcomes is the successful encapsulation of polyaniline, polythiophene, and polyacetylene copolymers within

PAMAM dendrimers, which will enhance their stability, processability, and functionality for CBRN-related applications. This encapsulation process will be confirmed using various characterisation techniques such as FTIR, XRD, SEM, and TEM. Additionally, the encapsulated conducting copolymers are expected to offer improved sensitivity and selectivity for the detection of chemical and biological warfare agents, enabling the development of advanced sensors. Furthermore, the project aims to create innovative protective coatings and materials for personal protective equipment (PPE) that offer better protection against a range of CBRN threats while maintaining comfort and flexibility for the wearer. Finally, the project is expected to lead to the development of novel gas filtration and decontamination materials with enhanced adsorption, neutralisation, or degradation capabilities for CBRN agents. Overall, the successful completion of this project has the potential to contribute significantly to the advancement of CBRN defence technologies, ultimately improving protection and detection capabilities.

The development and application of these encapsulated conducting copolymer nanocomposites could potentially revolutionise the CBRN defence industry, offering better protection and improved detection capabilities. The successful implementation of this project could lead to significant advancements in the field of CBRN defence, potentially saving lives and protecting critical infrastructure. Furthermore, the project could open up new avenues for research and innovation, contributing to the broader scientific community and defence industry.

ACKNOWLEDGEMENTS

I would like to express our sincere gratitude to everyone who directly or indirectly contributed to this project.

References

[1] J. B. Tucker and K. M. Vogel, 'Preventing the proliferation of chemical and biological weapon materials and know-how', The Nonproliferation Review, vol. 7, no. 1, pp. 88–96, Mar. 2000, doi: 10.1080/10736700008436797.

[2] L. Liu, Y. Yin, L. Hu, B. He, J. Shi, and G. Jiang, 'Revisiting the forms of trace elements in biogeochemical cycling: Analytical needs and challenges', TrAC Trends in Analytical Chemistry, vol. 129, p. 115953, 2020, doi: https://doi.org/10.1016/j.trac.2020.115953.

[3] 'APS -2008 APS March Meeting - Event - Synthesis and characterisation of erbium (III)-doped polyimide nanofibers for low temperature thermophotovoltaic applications', in Bulletin of the American Physical Society, vol. Volume 53, Number 2. Accessed: Mar. 16, 2023. [Online]. Available: https://meetings.aps.org/Meeting/MAR08/Session/C1.5

[4] H. Liu, J. Huang, J. Mao, Z. Chen, G. Chen, and Y. Lai, 'Transparent Antibacterial Nanofiber Air Filters with Highly Efficient Moisture Resistance for Sustainable Particulate Matter Capture', iScience, vol. 19, pp. 214–223, Jul. 2019, doi: 10.1016/j.isci.2019.07.020.

[5] S. Fahimirad, Z. Fahimirad, and M. Sillanpää, 'Efficient removal of water bacteria and viruses using electrospun nanofibers', Sci Total Environ, vol. 751, p. 141673, Jan. 2021, doi: 10.1016/j.scitotenv.2020.141673.

[6] K. Li and B. Liu, 'Polymer-encapsulated organic nanoparticles for fluorescence and photoacoustic imaging', Chem. Soc. Rev., vol. 43, no. 18, pp. 6570–6597, Aug. 2014, doi: 10.1039/C4CS00014E.

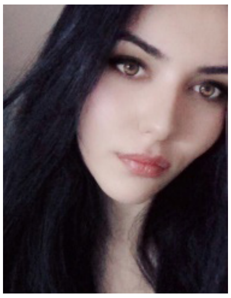
[7] M. Gide et al., 'Nano-Sized Lipidated Dendrimers as Potent and Broad-Spectrum Antibacterial Agents', Macromol Rapid Commun, vol. 39, no. 24, p. e1800622, Dec. 2018, doi: 10.1002/marc.201800622.

[8] K. H. Wong, Z. Guo, M.-K. Law, and M. Chen, 'Functionalised PAMAM constructed nanosystems for biomacromolecule delivery', Biomater Sci, vol. 11, no. 5, pp. 1589–1606, Feb. 2023, doi: 10.1039/d2bm01677j.

[9] D. J. Cardin, 'Encapsulated Conducting Polymers', Advanced Materials, vol. 14, pp. 553–563, Apr. 2002, doi: 10.1002/1521-4095(20020418)14:8<553::AID-ADMA553>3.0.CO;2-F.

[10] S. E, V. Jv, U. Šk, and L. A, 'Application of PAMAM dendrimers in optical sensing', The Analyst, vol. 140, no. 4, Feb. 2015, doi: 10.1039/c4an00825a.

Author



Elçin Tören holds a Ph.D. in Textile Engineering with a focus on Textile Technology from the Technical University of Liberec, where they also earned their Bachelor's and Master's degrees in the Department of Nanomaterials and Nonwovens. Their expertise lies in the intersection of textile engineering, biomaterials, and nanotechnology, with a particular emphasis on tissue engineering and drug delivery systems.

Elçin Tören has an impressive list of certifications and diplomas, including an Advanced Diploma in Tissue Engineering and a Principles of Drug Delivery Systems Diploma, both from CPD Certification Services. They have also completed numerous courses from renowned institutions like MIT and Middle East Technical University, covering topics such as biomaterials-tissue interactions, materials for biomedical applications, and various software and design tools.

Elçin Tören's skill set encompasses nano chemistry, biomedical engineering, material characterisation, nonwovens, nanomaterials, regenerative medicine, medical textiles, and anti-cancer drug research. They have a deep understanding of scaffold design, polymer science, human health, biocompatible materials, and hyaluronic acid applications.

With a passion for advancing the field of textile engineering and its applications in healthcare, [Your Name] is dedicated to researching and developing innovative solutions that have the potential to improve human well-being. Their work continues to inspire and pave the way for future advancements in the textile and biomaterials industries.

EUROPE'S DEFENCE: HOW DRONES CAN ENCHANCE COUNTERTERRORISM CAPABILITIES

Christos Chatzis[1], Xesfingi Eleni[2] and Karampelas Vasileios[3]

Abstract

The threat of violent radicalization is a complex and multifaceted challenge facing Europe. Drones are unmanned aerial vehicles (UAVs), designed to perform various tasks or missions. As drones continue to evolve, the legal and ethical issues surrounding their use, both in civilian and military contexts, pose challenges and uncertainties that require careful consideration and regulation, alongside effective counterterrorism strategies based on dynamic geopolitical factors among European Union (EU) member states. While a wide range of extremist groups have emerged, drones have played a role in reducing terrorist attacks, particularly in areas where ground troops are ineffective. This paper reviews the legal, ethical, and safety concerns associated with the use of counterterrorism drones in the EU, suggests a viable solution, and highlights the need for policymakers to carefully consider the long-term effects of their counterterrorism strategy and to ensure that drones' use is consistent with international law and human rights standards.

Keywords

Drones, Terrorism, Counterterrorism, European Union (EU).

1. INTRODUCTION

1.1 HISTORY OF DRONES

The history of drones, also known as unmanned aerial vehicles (UAVs), can be traced back to the early 1900s. According to Keane and Carr [1] (2013), one of the earliest examples of unmanned aircraft was developed in 1916 by the American inventor Charles Kettering. The drone, named the Kettering Bug, was designed for use as a weapon and was powered by a four-cylinder engine. However, the Kettering Bug was not used in combat due to technical issues and the end of World War I.

Blom [2] (2010) provides a comprehensive historical perspective on unmanned aerial systems. The author notes that the first successful drone flight was carried out in 1935 by the British Royal

Navy. The drone was designed for reconnaissance purposes and was used during World War II. In the following decades, drones were mainly used for military purposes, such as surveillance, target practice, and gathering intelligence.

In recent years, drones have become increasingly popular in both the military and civilian sectors. According to Army Technology's timeline [3] (2021), the use of drones in the aerospace and defense industry has rapidly evolved since the 1990s. With advancements in technology, drones have become smaller, more affordable, and easier to use. This has led to a wider range of applications, such as aerial photography, search and rescue, delivery, and agricultural monitoring. As drones continue to evolve, there is a growing need to address legal, ethical, and safety concerns associated with their use.

[1] HED Engineering, Athens, Greece hatzis@hed-engineering.com
[2] HED Engineering, Athens, Greece info@hed-engineering.com
[3] HED Engineering, Athens, Greece info@hed-engineering.com

1.2 ADVANTAGES

UAVs, offer several advantages in military operations, and their use has increased significantly in recent years. One major advantage is their ability to conduct surveillance and intelligence-gathering missions without putting human pilots at risk. Mahadevan [4] (2010) notes that drones can loiter over target areas for extended periods, providing persistent surveillance capabilities that manned aircraft cannot match. Additionally, UAVs can be equipped with high-resolution cameras and other advanced sensors that can provide real-time video feeds and other critical intelligence to commanders on the ground. This allows for quicker and more informed decision-making in military operations.

Another advantage of drones is their cost-effectiveness. Compared to traditional manned aircraft or ground-based vehicles, drones are less expensive to operate and maintain. This makes them a cost-effective option for many military and security operations. Drones can be used for various purposes, such as border patrols, monitoring wildlife, tracking natural disasters, and delivering emergency medical supplies to remote locations, among others. As technology advances, the cost of drones is likely to decrease further, making them more accessible and affordable for various applications.

Furthermore, drone technology has their ability to carry out precision strikes against targets with minimal collateral damage. Fields [5] (2012) notes that drones can be equipped with advanced targeting systems, such as laser-guided missiles, that can accurately hit a target with pinpoint accuracy. This precision allows for more targeted strikes that minimize damage to civilian infrastructure and avoid civilian casualties. Horowitz et al [6] (2016) also point out that drones can conduct targeted killings of high-value targets with minimal risk to military personnel, as demonstrated in the successful operations against high-level terrorist leaders in Yemen and Pakistan.

Finally, the autonomy of drones is a significant advantage. Fields [5] (2012) highlights the potential for drones to operate independently, using artificial intelligence and machine learning to analyze data and make decisions. This autonomy could enable UAVs to carry out complex missions without direct human supervision, such as reconnaissance, target acquisition, and even strike operations. This would increase the effectiveness and efficiency of military operations, while also reducing the risk to human personnel.

In conclusion, drones offer numerous advantages in military operations, including persistent surveillance capabilities, precision strikes, and the potential for autonomous operations. While there are also limitations and ethical considerations surrounding the use of drones, their advantages have made them an increasingly valuable tool in modern warfare.

Drones can be used in various ways. They have a number of advantages that make them useful for various applications, including military, civilian, and commercial.´ he advantages of drones are described on the following paragraph. In summary, their advantages are cost-effectiveness,

flexible and versatile, safety for personnel, accessibility, precision and reduced environmental impact.

1.3 DISADVANTAGES

On the other hand, drones have their disadvantages. One major concern is the potential for collateral damage during drone strikes. The use of drones has been criticized for causing civilian casualties and property damage, leading to public outrage and negative perceptions of the technology. The study by Horowitz et al. [6] (2016) emphasizes the importance of separating fact from fiction in the debate over drone proliferation, as misconceptions about the effectiveness and accuracy of drone strikes can lead to unintended consequences and undermine public support for counterterrorism efforts.

Another limitation of drones is their susceptibility to technical issues and limitations in their capabilities. For instance, drones may encounter difficulties in adverse weather conditions, such as strong winds or heavy rain, which can affect their flight performance and ability to collect data. In addition, the range and flight time of drones are limited, which can hinder their effectiveness in long-term surveillance or monitoring operations. Furthermore, the legal and ethical issues surrounding the use of drones, both in civilian and military contexts, pose challenges and uncertainties that require careful consideration and regulation. Mitrea's [7] (2020) study highlights the need for a comprehensive framework that addresses the ethical and legal issues associated with drone technology to ensure its responsible use and minimize potential risks and negative impacts.

2. TERRORISM IN EU

2.1 HISTORY OF TERRORISM IN EU

The history of terrorism in the European Union (EU) has been shaped by a complex set of political, economic, social, and cultural factors. According to [8] Bjørgo (2004), the root causes of terrorism in the EU are multifaceted and cannot be reduced to a single factor. Instead, they are the result of a combination of factors, including political grievances, economic disparities, social marginalization, and cultural differences. Bjørgo [8] argues that these factors have created an environment that is conducive to the emergence and proliferation of terrorist groups in the EU.

Horgan (2004) [9] emphasizes the psychological dimension of terrorism, arguing that individuals who engage in terrorist activities often do so as a result of a complex set of personal, social, and political factors. According to Horgan, many terrorists are motivated by a sense of anger, frustration, and injustice, which they channel into violent acts. Moreover, he argues that terrorists often have a deep sense of commitment to their cause, which makes them willing to take extreme measures to achieve their goals. This psychological dimension of terrorism has played an important role in shaping the history of terrorism in the EU, as it has contributed to the emergence of a wide range of extremist groups and individuals who are willing to resort to violence to achieve their objectives.

Silke [10] (2003) emphasizes the importance of research in understanding the nature and causes of terrorism in the EU. He argues that research can help policymakers and law enforcement agencies develop effective strategies for preventing and countering terrorism. Moreover, he suggests that research can help us to better understand the underlying causes of terrorism and to identify the key factors that contribute to its emergence and proliferation. Silke's work highlights the need for ongoing research into the history of terrorism in the EU, as well as the need for greater collaboration between scholars, policymakers, and law enforcement agencies to address this complex and multifaceted phenomenon.

2.2 THE CONTRIBUTION OF DRONES AGAINST TERRORISM

The use of drones in counterterrorism has been the subject of much debate and controversy. While some argue that drone strikes are a necessary and effective tool in the fight against terrorism, others criticize their legality and ethical implications. Johnston and Sarbahi [11] (2016) examined the impact of US drone strikes on terrorism in Pakistan between 2004 and 2013. They found that drone strikes did indeed reduce the number of terrorist attacks in Pakistan, particularly those carried out by the Pakistani Taliban. However, they also found that drone strikes were associated with an increase in attacks by other militant groups, such as the Haqqani network. The authors argue that this unintended consequence of drone strikes underscores the need for policymakers to carefully consider the long-term effects of their counterterrorism strategies.

Jang [12] (2013) makes a case for the lawfulness of combat drones in the fight against terrorism. He argues that drones are a necessary tool in the modern battlefield, as they provide intelligence, surveillance, and reconnaissance capabilities that are critical in identifying and targeting terrorists. Jang contends that drones are subject to the same legal and ethical considerations as traditional weapons systems and that they are a more humane option than traditional ground combat, as they can be used to target specific individuals rather than indiscriminately targeting entire populations. However, he also acknowledges that the use of drones raises concerns about civilian casualties and the potential for abuse, and he argues that policymakers must ensure that drones are used in a manner that is consistent with international law and human rights standards.

Although drones have played a role in reducing terrorist attacks, particularly in areas where ground troops may not be able to operate effectively, they also highlight the need for policymakers to carefully consider the long-term effects of their counterterrorism strategies and to ensure that drones are used in a manner that is consistent with international law and human rights standards.

2.3 GEOPOLITICAL ANALYSIS

The rise of violent radicalization in Europe is a growing concern for policymakers and law enforcement agencies. According to Dalgaard-Nielsen [13] (2010), understanding the factors that contribute to violent radicalization is crucial to developing effective counterterrorism strategies. In particular, there is a need to distinguish between various forms of radicalization, including religious, political, and social, in order to address their underlying causes.

Dempsey and McDowell [14] (2019) provide insights into the complex geopolitical factors that have contributed to Europe's migration crisis. Their study highlights how the media's portrayal of disasters and crises, such as the refugee crisis, can shape public perceptions and fuel anti-immigrant sentiment. This, in turn, can create an environment that is conducive to violent radicalization.

The European Union's Strategic Compass [15] (2021) sets out a framework for addressing security threats, including terrorism. EU emphasizes the importance of addressing the root causes of terrorism, including political instability, economic factors, and social and cultural factors. It also highlights the need for greater cooperation between EU member states in sharing information, intelligence, and best practices for countering violent extremism.

The key geopolitical factors that have contributed to the rise of terrorism in the EU can be summed into the following factors:

1. Political instability
2. Economic disparities, poverty, and unemployment
3. Social and cultural alienation, discrimination, and differences
4. Geographic proximity to conflict zones in the Middle East and North Africa
5. Technological advances in communication and recruitment through the internet and social media.

Effective counterterrorism strategies must consider the geopolitical factors mentioned above. EU member states must also address the complex interplay between media portrayals of disasters and crises, public perceptions, and anti-immigrant sentiment. Finally, it there must be a common understanding and cooperation among EU member states in addressing the root causes of terrorism and countering violent extremism.

In conclusion, the threat of violent radicalization is a complex and multifaceted challenge facing Europe. By taking a comprehensive and coordinated approach, policymakers and law enforcement agencies can develop effective strategies for countering the threat of terrorism and promoting social cohesion and stability in the region.

3. COUNTERTERRORISM DRONE

3.1 PURPOSE

As mentioned above, drones can play an important role in counter-terrorism efforts. The purposed drone is intended for multirole purposes. Multirole drones, also known as versatile drones, are unmanned aerial vehicles (UAVs) that are designed to perform various tasks or missions, rather than being specialized for a specific purpose.

3.2 KEY ADVANTAGES

Multirole drones offer several key advantages that make them a valuable asset in counter-terrorism operations. Firstly, they provide flexibility and versatility as they can be used for a range of tasks including surveillance, reconnaissance, and search and rescue operations. Additionally, they offer improved situational awareness, allowing for real-time information to be gathered and enhancing response times to threats. This makes them a valuable tool in identifying potential threats and effectively responding to them.

Multirole drones also provide significant time-saving benefits. They can be rapidly deployed and respond quickly to critical situations, providing valuable support to counter-terrorism operations. Furthermore, their use reduces the risk to personnel as they can be deployed in hazardous environments or conflict zones where it may be dangerous or difficult to send personnel. This allows for safer operations and minimizes the risk to human life.

Finally, multirole drones are cost-effective as they can perform multiple tasks, reducing the need for specialized drones and saving money on logistics and maintenance. In summary, multirole drones offer numerous benefits that make them an essential tool in counter-terrorism operations, improving response times, situational awareness, and reducing the risk to personnel.

3.3 FUNCTIONALITY

By building upon a multirole platform, it is possible to extract the most out of a drone. Maximizing every drone's potential leads in maximizing resources spent on that particular area. Thus, operators can reduce their operating cost without sacrificing anything from the operational aspect. The amount of money that is being saved can be used with two ways. Either to reduce overall defense budget (importantly without any compromises) either to spent it elsewhere, on other defense sectors.

Below, it is described the drone's multipurpose functionality.

- **Intelligence gathering.** Drone can be equipped with cameras, sensors, and other equipment that can be used to gather intelligence on terrorist activities. This can help law enforcement agencies to identify possible terrorist activities. This can also help them to identify and track terrorists, monitor their movements, and plan operations to apprehend them.
- **Surveillance.** Drones can be used to conduct surveillance of high-risk areas, such as airports, train stations, and public events. They can provide real-time video feeds to security personnel, allowing them to detect suspicious activity and respond quickly.
- **Targeted strikes.** Drone can be used to carry out targeted strikes against terrorist targets. This can be done with precision-guided munitions, which can minimize collateral damage and reduce the risk to personnel.
- **Border security.** Drones can be used to monitor borders and prevent the movement of terrorists and their weapons across borders. They can be equipped with sensors to detect movement, and can quickly respond to any threats.
- **Search & rescue.** Drones can also be used to conduct search and rescue operations in the aftermath of a terrorist attack. They can be used to locate survivors and assess the damage to infrastructure, helping to speed up the recovery process.

Overall, a multirole drone can provide a valuable tool for law enforcement and counter-terrorism agencies. By providing real-time intelligence and surveillance capabilities, it can help prevent terrorist attacks and improve the response to incidents when they occur.

3.4 DRONE'S CHARACTERISTICS & CAPABILITIES

As seen above a multipurpose drone has the ability to assist or engage into many different scenarios. Because every scenario has its own demand in the equipment necessary, a modular design on the drone is the clear path to follow, along with compatible sensors for each and every scenario. The modular design expands also in the battery slot, as anyone can replace the old battery with a new one in a matter of seconds. That literally means that the multirole drone can adjust into a new, completely different scenario in less than a minute. All it takes is to replace the package of sensors with the desired one, for the purpose of the mission, and replace the old battery with a new one, so it can go from low charged to fully charged. All those features form a package of ultimate utility. It makes the whole operation easy, simple and fast.

Furthermore, the multirole drones can be supported by a mobile station. The mobile station could be a heavy-duty car made to assist and support the drones with their operations. Through the mobile station, service and maintain of the drones is possible from anywhere. Also, inside the station there can be a special compartment in which the sensors, for the various types of operations, and batteries are stored. Another capability of the mobile station could have, is the Flight Control Assistance of the drone. Through Flight Control Assistance the operator can access real-time data that the drone receives from its sensors, such as live image, sound and environment parameters. Thus, the Mobile Station is the platform, designed in order to maximize drone's operational ability.

Special operations require specific sensors, depending on the scenario. As described above the multipurpose drone has different packages of sensors for each different scenario.

Down below we describe the sensors used for every operation.

- **Intelligence gathering.** Equipped with 8K camera, Night Vision camera, Thermal camera, Material detection sensors, LiDAR map sensor, Laser HQ audio (LiDAR) sensors.
- **Surveillance.** Equipped with 4K camera with 20x Optical Zoom, Night Vision camera, Thermal camera, Material detection sensors, Biometric sensors, Laser HQ audio (LiDAR) sensors.
- **Targeted strikes.** Equipped with 8K camera, Night Vision camera, Thermal camera, Material detection sensors, Laser HQ audio (LiDAR) sensors, Laser-guided ammunition.
- **Border security.** Equipped with 4K camera with 20x Optical Zoom, Night Vision camera, Thermal camera, Material detection sensors, LiDAR map sensor, Movement detection sensors, Laser HQ audio (LiDAR) sensors.
- **Search & rescue.** Equipped with 4K camera with 20x Optical Zoom, Night Vision camera, Thermal camera, Laser HQ audio (LiDAR) sensors.

4. CONCLUSION

The use of drones in the aerospace and defense industry has rapidly evolved since the 1990s. UAVs, offer several advantages in military operations, and their use has increased significantly in recent years. As technology advances, the cost of drones is likely to decrease further, making them more accessible and affordable for various applications.

The rise of violent radicalization in Europe is a growing concern for policymakers and law enforcement agencies. Terrorism in the European Union (EU) is being shaped by a complex set of political, economic, social, and cultural factors. EU must not underestimate the importance of addressing the root causes of terrorism and act accordingly. Effective counterterrorism strategies should be considered among EU member states, based on the dynamic geopolitical factors.

Drones can play an important role in counter-terrorism efforts. Multirole drones offer several key advantages that make them a valuable asset in counter-terrorism operations. By providing real-time intelligence and surveillance capabilities, it can help law enforcement agencies prevent terrorist attacks and improve the response to incidents when they occur.

References

[1] Keane, J. F., & Carr, S. S. (2013). "A brief history of early unmanned aircraft", Johns Hopkins APL Technical Digest, Vol 32, No 3, pp558-571.

[2] Blom, J. D. (2010), "Unmanned aerial systems: A historical perspective", Fort Leavenworth, KS: Combat Studies Institute Press, Vol. 45.

[3] Drones in Aerospace and Defence: Timeline (army-technology.com)

[4] Mahadevan, P. (2010), "The military utility of drones", CSS Analyses in Security Policy, Vol 78.

[5] Fields, N. R. (2012), "Advantages and challenges of unmanned aerial vehicle autonomy in the Postheroic age".

[6] Horowitz, M. C., Kreps, S. E., & Fuhrmann, M. (2016), "Separating fact from fiction in the debate over drone proliferation", International Security, Vol 41, No 2, pp7-42.

[7] Mitrea, G., (2020), "Drones-Ethical and Legal Issues in Civil and Military Research as a Future Opportunity", Journal for Ethics in Social Studies, Vol 4, No 1, pp83-98.

[8] Bjørgo, T. (Ed.), (2004), "Root causes of terrorism: Myths, reality and ways forward", Routledge.

[9] Horgan, J. (2004), "The psychology of terrorism", Routledge.

[10] Silke, A. (Ed.), (2003), "Research on terrorism: Trends, achievements and failures", Routledge.

[11] Johnston, P. B., & Sarbahi, A. K. (2016), "The impact of US drone strikes on terrorism in Pakistan", International Studies Quarterly, Vol 60, No 2, pp203-219.

[12] Jang, H. D. (2013), "The Lawfulness of and Case for Combat Drones in the Fight Against Terrorism", Nat'l Sec. LJ, Vol 2, No 1.

[13] Dalgaard-Nielsen, A. (2010)., "Violent radicalization in Europe: What we know and what we do not know", Studies in conflict & terrorism, Vol 33, No 9, pp797-814.

[14] Dempsey, K. E., & McDowell, S. (2019), "Disaster depictions and geopolitical representations in Europe's migration 'Crisis'", Geoforum, Vol 98, pp153-160.

[15] European Union's Strategic Compass, 2021, "A STRATEGIC COMPASS FOR SECURITY AND DEFENCE" (https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

A MODULAR APP STORE REFERENCE ARCHITECTURE (MASRA)

Demetris Antoniou[1], Stylianos Koumoutzelis[1], Titos Georgoulakis[1], Emmanouil Kafetzakis[1], Ioannis Giannoulakis[1].

Abstract

The purpose of this paper is to present a reference architecture for the creation of an Interoperable AppStore (the "MASRA") which enables the delivery of additional value (operational benefits) by the combination of functionalities among its hosted applications. A set of operational, application, data and technology architectural principles are presented. In addition, a reference architecture is provided to demonstrate the implementation of the architectural principles.

Keywords

EDA Innovation, Interoperability, System Architecture.

1. INTRODUCTION

In contrast to commercial app stores which drive sandboxing between applications (such as those provided by commercial smartphone providers) MASRA is designed to promote interoperability between the hosted applications. Interoperable app stores such as the MASRA enable the solving of complex problems which would otherwise be impossible to solve by segregated applications. By combining the capabilities of each hosted application and generating a unified data flow higher levels of abstraction can be achieved.

Such solutions are especially relevant to military applications due to the blurring of military theatres, the role of information in modern warfare and the fluctuating conditions of the modern, multi-theatre battlefield. Moreover, interoperable information weapons enable cooperation between EU member state militaries and the leveraging of cross-European capabilities.

The European Defence Agency aims to further integrate the military capabilities of EU member states. Solutions, such as the MASRA, which promote the cooperation and capability- multiplication of various armed forces are key to the promotion of further integration.

This paper uses the TOGAF 9.2 [1] standard to identify the conceptual architecture of the MASRA across its constituent architectural layers and their resultant architectural principles. Finally, a reference architecture is presented using the ArchiMate modelling [2] language.

In summary, the MASRA serves as a collaborative platform for military purposes, bringing together various member states to contribute and utilize applications tailored to their specific needs. By fostering European collaboration and fostering a shared ecosystem of modular applications, this military focused MASRA aims to enhance the efficiency, adaptability, and overall effectiveness of defence operations across member states.

2. FUNDAMENTAL PRINCIPLES OF THE MASRA PLATFORM

To describe the MASRA and to achieve its intended outcome, a set of architectural layers have been developed based on the TOGAF 9.2. Each layer is defined by one fundamental architectural principle with its associated rationale and implications.

[1] 8Bells Research, Nicosia, Cyprus info@8bellsresearch.com

2.1. USER INTERFACE (UI) LAYER

Principle Name: Intuitive and user-friendly interfaces

Statement: Design and develop user interfaces that prioritize ease of use, clarity, and accessibility for diverse user groups.

Rationale: Providing intuitive and user-friendly interfaces enhances user satisfaction, improves productivity, and reduces the learning curve for new users. This principle aligns with the goal of delivering a high-quality user experience across the app store ecosystem.

Implications: Developing intuitive interfaces may require additional design resources, user research, and usability testing. User feedback should be continuously collected and analysed to improve interfaces over time.

2.2. API LAYER

Principle Name: Open and standardized APIs

Statement: Implement APIs based on open standards and provide comprehensive documentation to facilitate seamless integration and interoperability.

Rationale: Open and standardized APIs simplify integration, increase compatibility between applications and services, and reduce vendor lock-in. This principle supports the goal of creating a flexible and adaptable app store ecosystem.

Implications: Providing clear and thorough documentation may increase development time and resource requirements. Regular updates to APIs may be necessary to maintain compliance with evolving standards.

2.3. APPLICATION SERVICES LAYER

Principle Name: Modular and reusable services

Statement: Create application services that are modular, reusable, and extendable to promote flexibility and adaptability within the MASRA ecosystem.

Rationale: Modular and reusable services enable efficient development, reduced duplication, and easier maintenance. This principle aligns with the goal of creating a scalable and adaptable app store architecture.

Implications: Developers need to design and implement services with modularity and reusability in mind. This may increase initial development time but will result in long-term benefits.

2.4. INTEGRATION SERVICES LAYER

Principle Name: Seamless integration and extensibility

Statement: Enable seamless integration of third-party applications, services, and data sources while maintaining a flexible and extensible architecture.

Rationale: Seamless integration and extensibility facilitate the incorporation of new applications and services, enhancing the app store's overall capabilities and value. This principle supports the goal of fostering a robust and adaptable app store ecosystem.

Implications: Integration and extensibility must be considered during the design and development of applications and services. This may require additional development resources and time to ensure compatibility and adaptability.

2.5. DATA LAYER

Principle Name: Secure and scalable data management

Statement: Implement data management practices that ensure data integrity, security, and availability while supporting scalability.

Rationale: Secure and scalable data management practices protect sensitive information, prevent data loss, and support growth as the MASRA ecosystem expands. This principle aligns with the goal of maintaining a reliable and trustworthy app store.

Implications: Robust data management practices must be implemented, requiring additional resources and effort. Regular audits and monitoring of data practices may be necessary to ensure compliance with this principle.

2.6. SECURITY LAYER

Principle Name: Defence in depth

Statement: Employ a multi-layered approach to security, incorporating measures at the application, infrastructure, and data levels to safeguard the app store ecosystem from threats.

Rationale: A defence in depth strategy ensures comprehensive protection against security threats, reducing risks and enhancing the app store's overall trustworthiness. This principle supports the goal of maintaining a secure and reliable app store.

Implications: Implementing a defence in depth strategy requires additional resources, expertise, and ongoing monitoring. Security measures must be regularly evaluated and updated to address emerging threats.

2.7. INFRASTRUCTURE LAYER

Principle Name: Scalable and resilient infrastructure

Statement: Provide a scalable and resilient infrastructure capable of handling fluctuations in demand and recovering quickly from failures.

Rationale: A scalable and resilient infrastructure ensures the app store remains accessible, performant, and reliable even under changing conditions. This principle aligns with the goal of delivering a high-quality and dependable app store experience.

Implications: Building a scalable and resilient infrastructure may require additional investment in hardware, software, and expertise. Regular monitoring and maintenance are necessary to ensure continued performance and resilience.

2.8. ETHICS LAYER

Principle Name: Ethical compliance and responsibility

Statement: Ensure applications and services adhere to ethical guidelines, legal regulations, and military standards.

Rationale: Upholding ethical compliance and responsibility demonstrates commitment to high standards, fosters trust among users, and mitigates potential risks associated with unethical practices. This principle supports the goal of maintaining a responsible and reliable app store ecosystem.

Implications: Ethical compliance and responsibility must be integrated into the development, deployment, and maintenance of applications and services. This may involve additional resources, training, and oversight.

2.9. PRIVACY LAYER

Principle Name: Privacy by design

Statement: Integrate privacy considerations into the design and development process to ensure compliance with privacy regulations and protection of user data.

Rationale: Privacy by design helps safeguard user data, meet regulatory requirements, and foster trust among users. This principle aligns with the goal of delivering a secure and privacy-conscious app store experience.

Implications: Privacy considerations must be incorporated into the design and development of applications and services. This may require additional resources, expertise, and ongoing monitoring.

2.10. PERFORMANCE AND ANALYTICS LAYER

Principle Name: Data-driven decision-making

Statement: Leverage performance data and usage metrics to enable continuous improvement, informed decision-making, and better understanding of user behaviour.

Rationale: Data-driven decision-making supports evidence-based improvements, enhances app store capabilities, and helps tailor the user experience to better meet user needs. This principle supports the goal of creating a continuously evolving and adaptable app store ecosystem.

Implications: Systems for collecting, processing, and analysing performance data and usage metrics must be implemented. This may require additional resources, expertise, and infrastructure. Regular review of performance data and usage metrics is necessary to drive informed decision-making and improvements.

3. A REFERENCE ARCHITECTURE FOR MASRA

A reference architecture has been developed for the proposed MASRA which integrates and operationalizes the principles and layers indicated in the previous section. The reference architecture includes the defined layers and their governing principles. Note that this conceptual reference architecture does not include the relationships between elements.

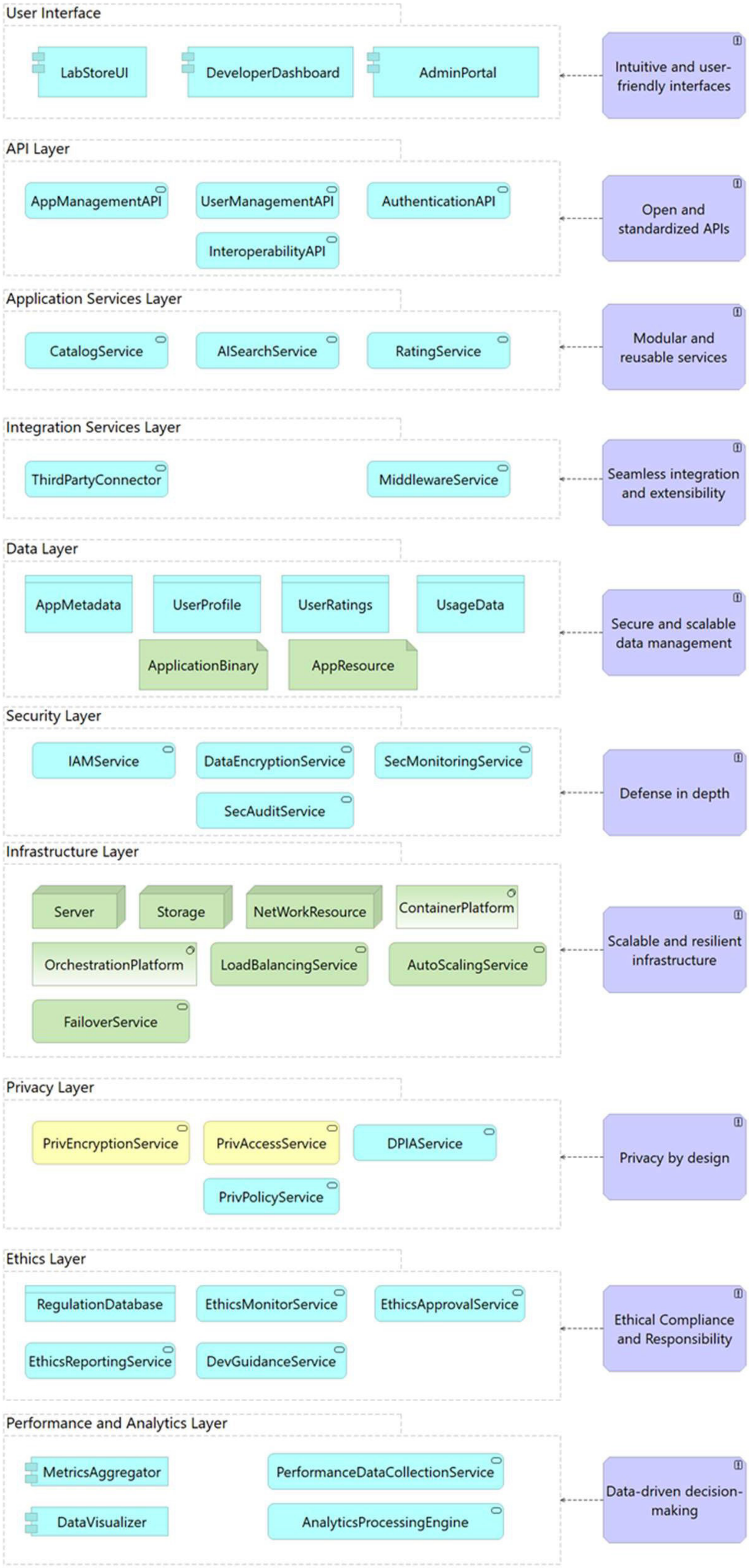


Figure 1: Reference Architecture (excluding relationships)

The above reference is to be a starting point for the design and implementation of MASRA. The above elements demonstrate the functionalities that should be provided by MASRA itself to the hosted applications.

4. FEATURES OF THE MASRA PLATFORM

The principal nature of this entity, as implied by its name, is to serve as a repository of software tools which can be then subsequently utilized by end users of the European Defence Agency. Nevertheless, this platform will be more than a mere storage unit that an end user can only access, navigate and extract information, as an extensive range of features and capabilities will enhance user experience. Thus, its value as an asset for the defence community reaches far more in comparison with a common database component. To that end, in the spirit of this study, it is crucial to elaborately provide a comprehensive description of possible features and capabilities to be materialized during the development of such a platform.

4.1 COMPREHENSIVE SOFTWARE LIBRARY

The term CSL is rapidly engaging the market over the last few years, as software solutions constitute a major pillar in the online product ecosystem. The diversity of this ecosystem is vast, as Software as a Product and Software as a Service (SaaP, SaaS) solutions can be spotted in various fields, even if their connection to such tools is not as apparent, such as the field of medical processing of genome annotations [3] or analysing patterns in noises from highways [4]. This phenomenon, entangled with the already rapid advancements in the field of software solutions, constitutes many challenges for developers and enterprises both to keep up with the vast range of software products available. A European MASRA aims to resolve this situation, by providing a comprehensive platform for end users to access and share software solutions focused solely on defence applications, making it easier to manage and distribute such tools.

4.2 USER-FRIENDLY INTERFACES

This feature refers to the design and development of a user interface for the finalized and deployed application of the MASRA that is easy to use, navigate, and understand by the end-users. To ensure that the products contained and hosted in this platform are effective, the UI needs to be designed with the end-users in mind, making it intuitive and elaborate enough for them to navigate through the various components [5]. To achieve such a feature, several design principles need to be followed. First, the application needs to have a simple and consistent layout, with clear navigation and a logical structure. This will make it easy for users to find what they are looking for and understand how to use the tools available.

One of the main concepts of MASRA is to empower citizen developers to create and contribute to the platform in a creative way. As citizen developers, we refer to non-technical users who can create and share software applications using low code or no code development platforms. The suggested platform has a user-friendly interface and easy to use development and deployment tools that can help citizen developers create and share applications, thus enabling the platform to benefit from a wider range of solutions and foster innovation within the EDA community.

4.3 COLLABORATIVE ENVIRONMENTS/INTEROPERABILITY

As already mentioned, the tools available in this platform may be of some similarities, as they all focus on the defence projects market, but taken as standalone applications these tools create an ecosystem of various technological sectors. By thinking about those applications as building blocks, one can make well defined, robust and efficient combinations of such modules in order to create a higher level of implementation, which harnesses the advantages of each tool in order to create an elaborate, intricate new solution that can target a very specific need. To propose a very simple yet characterizing example, a deep fake video detector and an AI hate speech classifier can be interoperable by combining them in one module that performs anti-propaganda functionalities on social media platforms.

4.4 CUSTOMIZABILITY

Customizability can be a critical feature for the described platform, as the non-homogeneity described above ensures that unique needs are being met. By allowing customizability, the platform can cater to these unique needs by allowing developers to create apps tailored to the agency's requirements. Customizability additionally allows for flexibility in the design and development of applications, validating that they meet the specific needs of users. This flexibility can also help the adaptation to real-time changes of an ongoing operation that utilizes the MASRA. Customizable user profiles and apps can provide a better experience by allowing users to tailor the application to their specific needs and preferences.

4.5 SECURITY AND RELIABILITY

Security and this Reliability [6] is capable of ensuring the confidentiality, integrity and availability of the system's stored data. In order to achieve this, several features have been incorporated into the platform. An Identity and Access Management Service has been included to provide robust authentication and authorization mechanisms for user accessing the platform which ensures that only authorized personnel are eligible to have access to the data. Additionally, all data stored in the platform are encrypted to protect it from unauthorized access and data breaches. Furthermore, a Security Monitoring Service has been implemented to continuously monitor the platform for any security incidents or anomalies.

4.6 ANALYTICS AND REPORTING

This feature aims at providing insights about the usage and performance data of the software tools hosted on the platform. It will enable end users and administrators to track trends, identify areas of improvement while making data driven decisions about the selection and utilization of software tools. In addition, this feature will leverage data visualization modules, metrics aggregators and analytics processing engines in order to present data in an easily understandable format, leading to quicker and more informed user decisions. Furthermore, a Decision Support Service will offer guidance on improving the performance of these software tools based on data analysis.

6. ADVANTAGES AND DISADVANTAGES OF MASRA

The MASRA introduces several benefits to defence users. It **drives Innovation** by allowing non- technical users to combine functionalities of the hosted applications. Allows for **citizen developers** to create their own unique functionalities. It is **adaptable to battlefield needs** as it can rapidly adapt to changing conditions.

However, it also has several limitations [7]. Developers have additional requirements to add their applications to MASRA which increases development cost. It might violate legal and/or privacy considerations given that multiple applications are hosted which might have differing designs on privacy and compliance. This requires that MASRA is centrally hosted, applications are reviewed before publishing and periodic reviews are conducted on hosted applications. Furthermore, common use platforms increase their attack surface which necessitates the implementation and staffing of a security posture.

7. USE CASE: COLLECTING AND ASSESSING POTENTIALLY FAKE NEWS

The following use-case demonstrates how MASRA can assist the collection, fact-checking and visualization of fake news. This is achieved by combining three applications found on MASRA. First, the "News Aggregator" which collects information from the web (social media, news sites, privileged channels). Second, the "Fact-Checker" which analyses the collected information, verifies its credibility (using third-party fact checking services) and assigns a trustworthiness rating. Finally, the "News Dashboard" visualizes the information in a way that can be consumed by users and shared with others. In italics the relevant reference elements of MASRA are used.

Description: Develop and integrate a suite of interoperable fact-checking applications within the modular military app store to help users verify the credibility of news and information shared across military communication channels and civilian social media sources.

Steps:

Military personnel (users) access the military app store through the *WebAppStoreUI*.

Users open the News Aggregator application and set their preferences for news sources, including military communication channels and civilian social media platforms.

The News Aggregator connects with various trusted sources and databases through *ThirdPartyConnector* and *MiddlewareService* in the Integration Services Layer. The News Aggregator retrieves news and information from the selected sources.

The News Aggregator sends the collected data to the Fact-Checker application using *InteroperabilityAPI*.

The Fact-Checker application analyzes the received news data, verifies the credibility, and assigns a trustworthiness score to each news item. The Fact-Checker app uses its own algorithms and external fact-checking services through *ThirdPartyConnector*.

The Fact-Checker application sends the analyzed news items and trustworthiness scores to the News Dashboard application via *InteroperabilityAPI*.

The News Dashboard application presents the aggregated news, fact-checking results, and trustworthiness scores to the user in a user-friendly interface.

REFERENCES

[1] The Open Group, The TOGAF Standard, version 9.2, The Open Group, 2018.

[2] The Open Group, ArchiMate 3.1 Specification, The Open Group, 2019.

[3] G. Gremme, S. Steinbiss and S. Kurtz, "GenomeTools: A Comprehensive Software Library for Efficient Processing of Structured Genome Annotations," IEEE/ACM TRANSACTIONS ON COMPUTATIONAL BIOLOGY AND BIOINFORMATICS, vol. 10, no. 3, 2013.

[4] R. A. Harris, L. F. Cohn and J. H. Graham, "Comprehensive Software Library for Highway Noise Analysis," Journal of Computing in Civil Engineering, vol. 9, no. 2, 1995.

[5] E. G. Nilsson, "Design patterns for user interface for mobile applications," Advances in Engineering Software, vol. 40, no. 12, pp. 1318-1328, 2009.

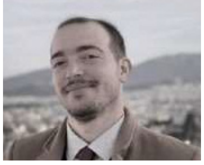
[6] M. Alenezi and I. Almomani, "Abusing Android permissions: A security perspective," 2017 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), 2018.

[7] J. Cowls, J. Morley and L. Floridi, "App store governance: Implications, limitations, and regulatory responses," Telecommunications Policy, vol. 47, no. 1, 2023.

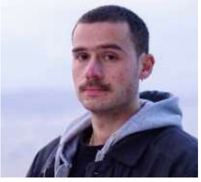
[8] A. Adomnita, "Balancing walled garden and open platform approaches for the IoT," 2016.

Authors

Demetris Antoniou is an experienced information security consultant having worked with major blue-chip organizations in the EU. His focus is on enterprise risk management, security strategy, risk assessments and corporate security transformations. With his Enterprise Architecture knowledge, Demetris has contributed to large-scale technology transformation projects and governmental studies on digital enterprise.



Stylianos Koumoutzelis is a graduate of the Electrical and Computer Engineering School of the National Technical University of Athens and has a strong foundation in both electrical engineering and computer science. With a focus on hardware design and development, he possesses expertise in the design and implementation of complex systems. He has also worked extensively in the fields of AI/ML, Telecommunications, and European research projects. His excellent analytical and problem-solving skills,



Titos Georgoulakis studied at the University of Patras - School of Engineering, where he majored in Electrical and Computer Engineering with a focus on Information Technology. Titos successfully completed his studies in April 2022 earning his Master of Engineering degree. He is currently being employed at Eight Bells, an independent high-technology company providing innovative solutions, as a research and development engineer.

Dr Ioannis Giannoulakis received his PhD from the National Technical University of Athens, Greece in applied mathematics. By leveraging on the collaboration with telecom operators, regulators, manufacturers, and academics he has built a strong background in the ICT domain, and he has been extensively involved in national and European research activities. In 2016 he founded 8BELLS Ltd, a dynamic research and consulting company with strong involvement and expertise in the areas of 5G mobile communications and cybersecurity.

Dr Emmanouil Kafetzakis is Co-founder of 8BELLS Ltd. Since 2002 he holds the BSc degree in Informatics and Telecommunications from the University of Athens, Greece, he also received his MSc and PhD degrees from the same university, in 2004 and 2011. Emmanouil has more than 15 years of experience working with operators, enterprises, and academics across Europe.

THE STRATEGIC PROMISE OF DIGITAL TWINS TO ENHANCE SUPPLY CHAIN RESILIENCE

Authors: Monica Adami[1], Mateusz Nowak[1], Maarten Toelen[1], Claudio Valle[1], Arno Van der hasselt[1], Annika Weinmann[1].

Abstract

In recent publications, the European Defence Agency has pointed out the need to make supply chains more resilient, a priority which was further highlighted by Russia's aggression against Ukraine. This paper argues that it is feasible to make (military) supply chains less redundant through the adoption of digital twins as a technological solution. Digital twins offer many advantages, above all real-time monitoring and analysis, which can strategically be combined with innovative crisis simulations and additional supporting technologies, to ensure supply chains survive in adverse and potentially unknown conditions, prevent supply shortages, reduce maintenance costs and time, and enable collaboration with other partners and stakeholders.

Keywords

Digital twins, Supply chain resilience, Data interoperability, Dual-use.

1. CONTEXT AND INTRODUCTION

In June 2018, the EDA's Capability Development Plan (CDP) underwent a significant revision, which resulted in the definition of 11 European capability development priorities, including *enhanced logistic and medical supporting capabilities*. Similarly, the Overarching Strategic Research Agenda (OSRA) defines common R&T priorities in the form of Technology Building Blocks (TBB), amongst which is the *Defence critical technologies supply chain* (TBB45). As illustrated by the ongoing war in Ukraine, military supply chains - and their resilience towards issues like challenging terrain, maintenance costs, availability of materials - have become crucial elements in defence. It has rightfully become an EDA priority to make military supply chains more resilient [1]. Building further upon this priority, this paper aims to explore a possible way forward to make military supply chains less redundant. In the context of supply chains, redundancy refers to having back-up systems, processes, or resources in place to ensure that operations can continue in the event of unexpected disruptions, for instance, due to an adversary offensive, natural disasters, geopolitical instability or equipment failures.

Digital twins are a key enabling technology that allow civil and military stakeholders to precisely simulate calamities and develop better and intelligence-driven decision-making in order to mitigate such crisis events. Identifying dependencies, bottlenecks and weaknesses in the provision of critical materials and assets - both primary and subsidiary - can also assist in better preparing resilience plans and strategies at a lower cost. In addition, through the usage of digital twins, civil and military stakeholders can monitor production processes, identify shortages or the absence of supply-chain diversification, in a timely and correct manner. Particularly in a domain such as military logistics, where high speed, fidelity and low fault tolerance are crucial, digital twins have a genuine potential to improve and facilitate military supply chains.

The operationalisation of digital twins in itself is no novelty however, as numerous examples of this innovative technology have already been adopted in (military) aviation [2]. In 2018, the Turkish Aircraft Industries Corporation entered an agreement with Siemens Product Lifecycle Management software to implement a complete digital twin in the company's manufacturing enterprise; in 2020, the US military used digital twin technology to improve planning and efficiency of F-35 fighter jets and Sikorsky UH-60 Black Hawk helicopters, and in 2021 Rolls Royce turned to digital twins to improve jet engine efficiency [3]. While this technology is already present in (military) aviation, there is vast untapped potential for it to be developed and implemented in other fields of the defence sector and

[1] PricewaterhouseCoopers Enterprise Advisory BV, Belgium arno.van.der.hasselt@pwc.com, maarten.toelen@pwc.com

scaled-up to the entire military supply chain - from a single (weapon) system to wider and more complex ones. The integration with other innovative technologies and processes such as 'internet of (military) things', blockchain and intelligence swarming combined with growing computing capabilities can make digital twins an operational reality. Digital twins of this kind would prove to be most effective in cases of cross-border supply chains in order to assess/ monitor feasibility of collaborations on international projects (e.g. EMBT or European Patrol Corvette) or in cases of crisis (e.g. humanitarian responses involving military operations, or supply of critical equipment/materiel to allies and partners such as Ukraine).

2. BUSINESS CASE

The military supply chain is a complex and multifaceted ecosystem that involves various interconnected processes such as the acquisition, storage, transportation, and distribution of equipment, supplies and military personnel. As illustrated by recent military operations, resilient and reliable supply chains are vital for societal resilience and to ensure operational effectiveness, whereas the current state of military supply chain management is often characterised by inefficiencies, redundancies and a lack of end-to-end visibility [4]. One of the key characteristics of military supply chains is their redundancy [5]. By having redundant systems in place, the military can minimise the impact of disruptions on their operations and ensure that goods and services continue to flow. However, redundancy can also lead to inefficiencies and unnecessary complexity if not managed properly. Maintaining excess inventory, for example, can tie up vital resources and increase costs, while having too many redundant suppliers can lead to unnecessary duplication of effort. As such, it is important to carefully balance the need for redundancy with the costs and risks associated with maintaining redundant systems.

2.1. REAL-TIME MONITORING AND ANALYSIS

Digital twins can provide real-time monitoring and analysis of the entire military supply chain, from suppliers to manufacturers, all the way to the end-user. They can thus be used to track inventory levels in real-time, providing a clear picture of which equipment is available and what needs to be replenished, as well as monitor the state of production and predict when maintenance is required. In turn, this would reduce downtime and augment the lifespan of equipment. By doing so, digital twins can help identify potential issues and bottlenecks in the supply chain, allowing for timely intervention to prevent disruptions. For instance, one of the main issues to take into consideration in relation to a military supply chain is the demand fluctuation, i.e., the variance in demand needs and/or budget. Military supply chains are exposed to large fluctuations in orders, going rapidly from orders of a few parts to large quantities, driven by optempo and unforecasted requirements. Taking this into consideration, military supply chains would benefit from the help of digital twins to facilitate end-to-end asset visibility, which ensures that supplies arrive at the right destination and time [6]. In other words, digital twins can support decision makers by providing them with precise and up-to-date information on the location and conditions of critical military supplies (food, fuel, weapons, equipment, and spare parts) and promptly react to meet operational needs. Outside of the European Union, one can identify numerous examples of digital twins being used to improve inventory management, repair and maintain military equipment, with the overall objective to optimise military operations. For example, the U.S. Army has developed a digital twin of its supply chain, called the Global Combat Support System-Army (GCSS-Army). GCSS-Army is a web-based logistics information system that provides real-time visibility into inventory levels, transportation status, and delivery times. It has been field-tested in various military operations, such as those in Iraq and Afghanistan, where it helped to reduce redundancies in the vast operational supply chain of the U.S armed forces. Another example of a digital twin is the U.S. Navy's Virtual Ship program, which provides real-time data on a Navy ship's systems and operations. This enables the Navy to optimise maintenance and repair schedules, proactively identify potential issues, and reduce downtime.

Whereas digital twins rely on the timely provision of reliable data to render an accurate supply-chain simulation and allow for meaningful scenario simulations, specific (organisational and legal) frameworks should be put in place to ensure that all key stakeholders across the supply chain share responsibility for data quality, especially when data has to be shared cross-border. However, the quality of data in military supply chain management can be variable due to several reasons, such as the complexity of the supply chain, the diversity of data sources and the challenges associated with (classified) data sharing and integration. Indeed, military supply chains involve multiple actors - including manufacturers, suppliers, logistics providers and end users, each with their own data systems and processes - and often operate in challenging environments, such as combat zones or disaster areas, which can affect the quality and availability of data. Legal frameworks can also provide a basis for the resolution of disputes related to data quality issues, as well as establish penalties for failing to meet data quality standards or for breaching agreements related to data management. Lastly, they can also encourage the adoption of best practices and standards for data quality across the supply chain. This can help to ensure that all parties have access to accurate and reliable data, which is essential for effective decision-making and efficient operations in military supply chain management.

2.2. SIMULATIONS

In crisis management, critical activities - such as the resilience of a supply-chain - are often subject to regular crisis exercises and testing. This can help military planners prepare for potential disruptions by making informed decisions based on the results of the simulations, developing contingency plans and evaluating their effectiveness. However, those exercises present a lot of drawbacks that reduce their efficiency over a vast military supply-chain: among other things, they are not frequent enough, not adjustable enough, too demanding and they are very expensive. In a fully functioning digital twin, changes in the physical world are directly translated into the virtual replica. The higher the quality of the data provided through sensors, 'internet of military things' and IT systems in general, the more accurate is the digital twin, its ability to provide snapshots of the current state and its ability to support simulations.

Through the convergence of crisis management with digital twins, military decision-makers could benefit from game-theoretic decision-making to improve situation assessment, facilitate multi-actor and cross-domain decision making, and increase coordination among various public and private stakeholders. Besides such macro-level advantages, crisis simulations can also be run to test the resilience of the digital environment - and parts of the supply chain - itself. Simulating a cyberattack and the interruptions in the supply chain caused by it, specific strategies and protocols can be prepared in order to minimise the impact. Having a digital replica and testing different scenarios, can allow for quickly spotting anomalies and detect if reality is matching some of those previously tested scenarios. In this sense, a digital twin has the potential to be used to prevent cyber-attacks by learning the behaviour of attackers and increase the security of the entire supply chain against cyber intrusions and malwares [7].

2.3. KEY SUPPORTING TECHNOLOGIES AND DATA INFRASTRUCTURES

Decentralised approaches to data processing such as 'edge computing' are pertinent in order to feed the digital environment with the necessary data flows. Edge computing is not a new concept in the military environment and has been successfully applied e.g. in the air domain, coupled with AI to gain military advantages based on information superiority [8]. This is the case of the F-35 which has unique capabilities to create networks among groups of aircrafts by combining information processed by each aircraft into a single stream of situational awareness and threat assessment. The scaling-up of edge computing to an entire supply chain environment allows for unprecedented data-driven strategic decision and long term policy-making. In such an environment, even if one node in the supply chain is disrupted, other nodes can continue to operate and provide critical data.

In combination with edge and decentralised computing, existing initiatives on data spaces can be crucial enablers for the pooling of the necessary data use in the digital twin environment. It is expected that in a few years, the European Commission will have successfully led the launch of common European dataspaces in several domains, including manufacturing and the supply chain or the Single European Sky, which has a clear potential to support military interoperability and coordination [9]. Overall, the combination of edge computing and data spaces can create a more distributed and resilient supply chain ecosystem, where data can be processed and analysed at the edge, while still being integrated into a centralised platform for overall supply chain management. Decentralisation of data collection and processing can make the digital twin more agile and feasible. By bringing computing power closer to the point of data generation, edge computing can reduce latency and improve the speed of data processing. In addition, such an approach can help in identifying new and mitigating the existing risks associated with data breaches and cyberattacks, which are major concerns in military supply chain management.

Moreover, by enhancing data availability and computing capabilities, progressive integration with advanced visualisation technologies can further support the optimisation of military supply chain processes and help limit redundancies. Mixed reality (MR) or extended reality (XR) applications in factories and military warehouses have the potential to provide a realistic simulation environment that allows users to interact with virtual objects and data in real time. For example, MR/XR applications can be used to simulate the placement of equipment and supplies in a military warehouse, enabling users to test different scenarios and optimise layouts for maximum efficiency. In addition, these applications can be used to simulate assembly lines and logistics operations in factories, allowing users to identify bottlenecks, improve workflows, and optimise resource utilisation [10].

2.4. EUROPEAN COLLABORATION

Initiatives such as *Sharing of Spare Parts* - aiming to manage spare parts for equipment and weapons systems across nations - have proven successful when it comes to collaboration across Member States in the field of military procurement and maintenance. More recently, the European Commission has adopted a proposal for a Regulation to establish the *European Defence Industry Reinforcement through common Procurement Act* for 2022-2024 [11], which is already being used to jointly procure support for Ukraine. Going one step further, digital twins can be used to share data and collaborate across different military units and organisations [2]. This could then improve communication and coordination, resulting in more effective supply chain management. By operationalizing digital twins, military organisations can facilitate a shared digital platform that provides real-time visibility into the entire military supply chain. In addition to providing a common operating picture for all stakeholders and this help reduce the duplication of efforts, digital twins - used in this manner - can facilitate data sharing by providing a secure space for sharing sensitive information. With the help of advanced encryption and access controls, digital twins can ensure that only authorised personnel have access to sensitive information, while enabling collaboration and information sharing.

Digital twins have already been used to improve collaboration and coordination between different teams involved in manufacturing processes. By creating a digital twin of a manufacturing process, designers, engineers, and production managers can work together more effectively to optimise production and reduce costs. By integrating digital twins into military supply chains, it will be possible to create virtual replicas of military logistics and supply chain systems, including transportation networks, warehouses, and distribution centres. As such, military logistics personnel from different units or branches can work together to optimise logistics and supply chain operations. Looking into the future, digital twins can foster collaboration but, in turn, they can be improved by collaboration and coordination at European level. To ensure timely data availability, ad hoc systems should be put in place to allow data sharing in secure and trusted environments. To this end, military supply chain data lakes and defence dataspaces could be developed at European level and become the backbone of digital twins, bringing together industry, governments and military structures.

The European Union can support the development of digital twins in several ways. The EU (also through the EDA) can provide funding and resources to support research and development of digital twin technologies. This can help to accelerate the development and deployment of digital twin solutions in conflict scenarios. The technical set-up of the digital twins must include clear approaches to data interoperability, which are at the very essence of data sharing, to ensure that they are interoperable and compatible across different industries and sectors. This means reusing existing standards and formats to ensure alignment with other initiatives (e.g. sectoral data spaces). In addition, the EU can invest in education and training programmes to develop the skills and knowledge necessary to design, develop, and operate digital twin solutions. This can help, for instance, to create a skilled workforce that can ensure high cybersecurity requisites for digital twins, which rely on connectivity and data exchange and are, therefore, vulnerable to cyber threats.

3. CROSS-DOMAIN APPLICABILITY

The relevance of digital twins also resides in their cross-sector nature and applicability. On the cross-military dimension, there are several systems needing the same type of components to be produced or to function. This is the case when it comes to the same types of microchips used to produce artillery targeting/guiding systems of ships, aircrafts and tanks or same type ammunition which could be deployed in different scenarios. An example of the latter is represented by the Aster missile which can be operated by different launching platforms such as the

FREMM frigates or the SAMP/T anti-air land system. Having an up-to-date view of production processes, stocks and location of military goods makes it possible to redeploy them as needed across interoperable systems, addressing pressing needs while allowing for the manufacturers to replenish stocks. This could prove particularly useful in conventional military and alliance operations, where large scale pooling of military resources across different countries put inventories and manufacturers under pressure. The emergency exposed relatively late widespread issues in production and supply chain capabilities which could have been pre-emptively detected through accurate and data-driven simulations.

In addition to the purely military dimension, a digital twin designed to support military supply chains has to also gather data from the manufacturing industry, from logistical services, and from critical service providers (e.g. energy). For instance, European manufacturers in many strategic fields are dependent on supplies of critical raw materials and intermediate goods for their production. These include for instance lithium, semiconductors and microchips which are crucial not only for the military systems, but also for the regular production of vehicles or electronic medical equipment, used in everyday life and crucial in times of crisis. This is also in line with latest EU policies such as the *Critical Raw Materials Act* which clearly states the need to ensure a secure and sustainable supply of raw materials for Europe's industry, which is at the core of the green transition, and in general to long-term European competitiveness and autonomy at world's level [12].

The preservation of minimum levels of strategic production capabilities is required to ensure that the supply chain of critical goods is constantly monitored and diversified. A digital twin would enable it to run simulations on supply shortages and cuts to key manufacturers and critical services, and preventively act to prepare contingency plans for uninterrupted supply chains.

Energy (both in terms of energy grids and fuels) is another case of critical supply chain which should be monitored for ensuring that the operativity of military installations and systems would not be altered in case of natural or man-caused adverse events. However, there are additional critical infrastructures which must be kept operational including not only hospital or government buildings, but also production lines and delivery of primary goods, from ammunition factories to food processing sites. Digital twins related to energy supply already exist and are used to inform decision making and support energy shortages responses. Pooling data on energy supplies into a broader security dimension, would allow them to extend their scope and support both military and civilian preparedness and resilience. It is therefore clear that the infrastructure needed to develop digital twins can also be kept in use in times of peace and be deployed to address and prevent issues which are specifically related to the military dimension.

4. CONCLUSIONS AND RECOMMENDATIONS

When considering operational lessons learnt from the Russian aggression against Ukraine, General Robert Brieger, Chairman of the EU Military Committee, highlighted that "logistics, often considered secondary compared to operational aspects, have once more demonstrated their crucial impact on warfare: footage of tanks out of fuel, kilometres-long convoys stalled on the street sides and soldiers hunting for food will fill history books with powerful images" [1]. In this regard, the importance of resilient and efficient supply chains in a military environment cannot be overstated. This paper proposes to use digital twins to make supply chains more resilient and efficient by reducing their redundancy, which is a characteristic inherent to all supply chains, military ones included. In particular, it suggests that it is possible to do so by exploiting the real-time monitoring and analysis of digital twins, combined with innovative crisis simulations, as well as leveraging collaboration strategies and the combined deployment of digital twins together with other key supporting technologies and data infrastructures.

The solution discussed in this paper consists of the creation of a digital twin at a much broader scale compared to what has been implemented so far. It consists of pooling together a massive amount of data which can support the monitoring of supply chain processes in both conflict time and in peacetime, for higher preparedness and resilience. This is achieved through a digital ecosystem monitoring production, shipments and stocks of critical goods which pools together data from a myriad of sources. Such data mass at the moment is not available or only partially, so it is suggested to create synergies with the Common European data spaces that are currently being launched in multiple domains by the EU. This would also allow the establishment of a 'modular' digital twin which can be plugged into a specific data space to retrieve data. This would be also beneficial for multiple reasons: i) obtain data at the necessary level of quality/granularity, ii) benefit from the governance and security requirements already in place, iii) benefit from decentralised computing.

Considering the current state and the expected growth in both high-quality data availability and computing capabilities, it is reasonable to assume a gradual development of this digital twin solution throughout the next two decades. In terms of computing capabilities, the current capabilities can already allow the digital twin not only for accurate descriptive analysis of the current environment and for conducting predictive modelling, but also for scenario planning and simulation. However, the real goal would be to move towards operational excellence based on real-time data integration through AI in control towers and possibly synced with advanced MX-based or XR-based data visualisation.

Meanwhile, with regards to data availability, this represents the main issue and highest efforts should be put in boosting it, both on the technical side and on the policy side. By the end of this decade, on the civilian side it can be expected that the first common EU data spaces will become operational and provide data useful for descriptive analysis and predictive modelling. On the military side, the same capabilities can be achieved if every country (individually or in joint ventures) starts the development of its own digital twins by pooling together data from warehouses and barracks, repair and training sites, ports/airports/missile sites, etc. This would be followed by extending the supply chain data flows, by plugging-in data from the defence industry. The result would be a 'defence data space' to be subsequently connected with other Common European data spaces (e.g. manufacturing) to complement the virtual supply chain with further data on other goods (e.g. medical supplies), energy and raw materials availability.

REFERENCES

[1] European Defence Agency (2022a). EDM Issue #23, EU's Strategic Compass / Follow the Ambition. Available at: https://eda.europa.eu/docs/default-source/eda-magazine/full-edm-23-(final).pdf.

[2] Bellamy III, W., (2018). Boeing CEO Talks 'Digital Twin' Era of Aviation. Aviation Today. Available at: https://www.aviationtoday.com/2018/09/14/boeing-ceo-talks-digital-twin-era-aviation/

[3] Mendi, A.F., Erol, T., and Doğan, D. (2022). Digital Twin in the Military Field, in IEEE Internet Computing, vol. 26, no. 5, pp. 33-40. Available at: https://ieeexplore.ieee.org/document/9345490.

[4] Sani, S., Schaefer, D., & Milisavljevic-Syed, J. (2022). Utilising Digital Twins for Increasing Military Supply Chain Visibility. Available at: https://eprints.lincoln.ac.uk/id/eprint/50348/.

[5] Katsaliaki, K., Galetsi, P. & Kumar, S. Supply chain disruptions and resilience: a major review and future research agenda. Ann Oper Res 319, 965–1002 (2022). https://doi.org/10.1007/s10479-020-03912-1

[6] Wu, J., Yang, Y., Cheng, X. U. N., Zuo, H., & Cheng, Z. (2020, November). The development of digital twin technology review. In 2020 Chinese Automation Congress (CAC) (pp. 4901-4906). IEEE.

[7] Holmes, D., Papathanasaki, M., Maglaras, L., Ferrag, M. A., Nepal, S., & Janicke, H. (2021, September). Digital Twins and Cyber Security–solution or challenge?. In 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). IEEE.

[8] Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2019). Edge intelligence: Paving the last mile of artificial intelligence with edge computing. Proceedings of the IEEE, 107(8), 1738-1762.

[9] SESAR Joint Undertaking (2020). Digital European Sky Blueprint. Available at: https://www.sesarju.eu/sites/default/files/documents/digital%20european%20sky%20blueprint.pdf

[10] PwC (2022). How digital twins can make smart cities better - Real-time simulations can create a bridge between physical and virtual worlds. Available at: https://www.pwc.com/m1/en/publications/documents/how-digital-twins-can-make-smart-cities-better.pdf

[11] European Defence Agency (2022b). EDM Issue #24, Investing in European defence today's promises, tomorrow's capabilities?, Available at: https://eda.europa.eu/docs/default-source/eda-magazine /edm24final.pdf.

[12] European Commission (2023). European Critical Raw Materials Act. Infographic. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1661

DESIGN AND DEVELOPMENT OF THE NEXT GENERATION, LOW-COST AND HIGH-SENSITIVITY HYDROPHONE FOR CRITICAL UNDERWATER INTELLIGENCE APPLICATIONS

Nefeli Motsi[1,2], Georgia Stamou[1,2], Spyridon Angelopoulos[1,2] and Evangelos Hristoforou[1,2,*].

Abstract

Hydrophones are used for various underwater acoustic applications. They can be stationary or portable, operating individually or as a part of large arrays. There are many factors, such as the harsh environmental conditions and the range of the acoustic signals, that lead to challenges during the development and evaluation of the hydrophones. All the above usually increase the cost or decrease the quality and robustness of the commercially available hydrophones. In this paper, the development of a low-cost hydrophone operating at a frequency range of 0.1 Hz to 100 kHz, is presented. Moreover, an electronic circuit was designed and prototyped, to improve hydrophone's performance and digitize its output, in order to perform further signal analysis through a personal computer. More specifically, the circuit includes a stage of preamplification, a stage of DC biasing, a stage of Analog-to-Digital Conversion and a microcontroller, in order to receive a digitized signal and analyze it, using specialized audio software. Finally, the hydrophone was calibrated using the substitution method, where its acoustic response was compared with that of a commercial one's. This EU-designed and developed hydrophone can already be used for a variety of Underwater Intelligence, Surveillance and Reconnaissance (ISR) missions (e.g. protection of underwater critical infrastructure such as pipelines, cables etc.) in a fixed or moveable deployment onboard Autonomous Vehicles (surface or underwater).

Keywords

hydrophone, piezoelectric material, hydrophone calibration, microcontroller.

1. INTRODUCTION

The study of underwater electroacoustic transducers, which have numerous applications such as sounding, bottom mapping, fish finding, investigation of ship and aircraft wrecks, oil exploration, and various research projects, involves a range of disciplines including mechanics, electronics, optics, magnetics, semiconductors, and acoustics [1,2]. These transducers convert acoustic pressure to electronic and vice versa, taking the form of underwater projectors and hydrophones in place of speakers and microphones, respectively, in air [2]. Thus, they can be used for recording or listening underwater sounds for civil and military purposes [3]. Acoustic waves are simply sound waves in any medium, and specifically in water they are transmitted as waves caused by the movement of water molecules. The main parameters of an acoustic wave are its pressure and frequency. Hydrophones, or hydrophone arrays, detect the pressure variations of acoustic waves within a certain frequency range, and convert this information into electric or optical signals. By analyzing these signals, the presence and other characteristics of a target can be determined [4].

The specific characteristics of each underwater transducer can only be accurately determined through measurements [5]. There are several techniques that can be used to calibrate hydrophones, including reciprocity, substitution methods, planar scanning, time delay spectrometry (TDS), vibrating column method and optical interferometry [6-9]. Each method has its own advantages and disadvantages, regarding its precision, whether it

[1] School of Electrical and Computer Engineering, National Technical University of Athens, 15780 Athens, Greece

[2] SOTIRIA Technology*, 10431, Athens, Greece (partnership) hristoforou@ece.ntua.gr, info@sotiria.tech

provides a direct or indirect determination, speed, frequency range, and whether it requires a free-field environment or just a laboratory tank.

Among piezoceramic materials, lead zirconate titanate (PZT) compounds are frequently used in underwater acoustic transducers, as they enhance the acoustic sensitivity and consequently the acoustic response of hydrophones [10,11,12]. Over time, the development of suitable piezo materials for underwater applications is constantly an active area of research.

In the marine industry, there is a need for a low-cost, energy-efficient underwater acoustic sensor, which would bundle not only the sensing element, but also the required electronics (i.e., preamplifier, ADC, microcontroller, etc.), to produce a digital output signal, suitable for long-distance transmission. In this way, the sensor will be able to be placed underwater as an autonomous device, giving the ability to analyze the received signals, and get more information about the sound source, its location and its frequency [13,14,15]. Thus, there will be a better perception of the underwater life through an economical construction, which is easy to install and supply.

In most works reported in the literature, though, the development of such a system stops at the construction of the sensing element, using commercial electronic devices for signal processing purposes, and sending the output to some data analysis platform [16]. The primary goal of this article is to present the design and development of an entire acoustic system that involves all of the aforementioned components (sensing element, electronics, packaging, hardware and software signal processing pipeline) using low-cost components. The proposed system is easy to manufacture, it presents high sensitivity at a wide spectrum which ranges from 0.1 Hz to 100 kHz, and facilitates both real time, as well as offline signal processing.

2. MATERIALS AND METHODS

In the beginning of this work, conventional off-the-shelf PZT ($Pb[Zr_xTi_{(1-x)}]O_{3\ 0\leq x\leq 1}$)) ceramic discs were used as acoustic transceivers. The sensing element consists of the ceramic disc, the required wiring, proper packaging with liquid rubber sealant to secure its waterproofness, as well as the corresponding electronics. Their calibration was realized by submerging them into a 3% saltwater tank, according to the estimated salinity of seawater, and monitoring their response by comparison with a commercial non-EU reference hydrophone [17]. Furthermore, they were used in pairs as transmitters and receivers, using a sinusoidal input signal of 20 V_{pp}, at different frequencies varying from 0.1 Hz to 200 kHz.

2.1 HYDROPHONE DESIGN AND DEVELOPMENT

Experimental hydrophones were produced as follows: A 3D-printed enclosure (Figure 1a) was designed and manufactured to house to protect the piezoelectric disk. For each PZT disc, two wires were soldered to the metal and piezoelectrical part, respectively (Figure 1b).

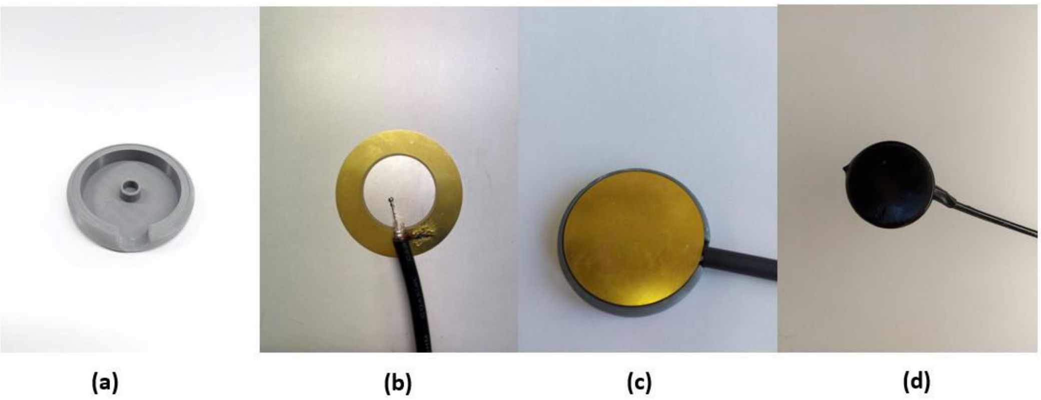


Figure 1. Hydrophone's development: (a) 3D-printed enclosure; (b) PZT sensing element with its wires soldered.; (c) PZT sensing element on the 3D-printed enclosure; (d) Final form, covered with liquid rubber sealant.

Afterwards, a weight was added into the 3D-printed enclosure to ensure its submersion. Finally, the entire structure was covered with liquid rubber sealant, in order to become waterproof when dry (Figure 1d). Figure 2 illustrates the final form of the developed hydrophone, terminated to a BNC connector, ready to be tested using either a preamplifier (using an appropriate adaptor, if needed), or an oscilloscope.

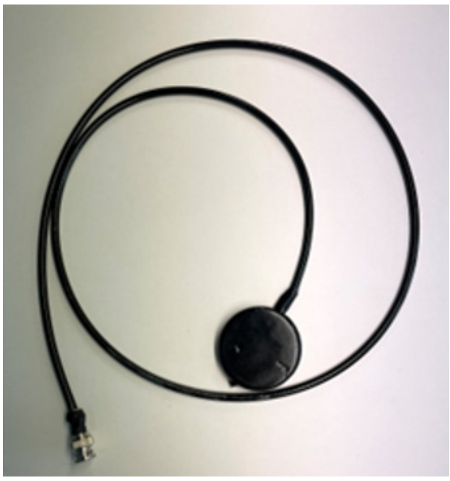


Figure 2. The developed hydrophone, including a cable and a BNC connector.

2.2 CALIBRATION TECHNIQUE

Substitution method was used in order to calibrate the hydrophone. More specifically, two transducers were submerged into a tank filled with water consisting of 3% salt, each one facing directly the other at a distance of 30 cm. One of the devices was used as a speaker and the other one as a receiver. The speaker was supplied by a 20 Vpp sinusoidal signal, having a frequency of 0.1 Hz to 200 kHz, while the receiver's output signal was observed through an oscilloscope. Later on, the lab hydrophone was replaced by the commercial one, while keeping the conditions of conducting the experiment and the entire set-up the same.

2.3 DESIGN AND DEVELOPMENT OF SENSOR'S ELECTRONICS

As mentioned above, hydrophones convert underwater sound signals into electrical signals, providing important information about the underwater environment and its changes. In many cases, it is necessary to detect distant and weak signals, eliminate the ambient noise, and transmit the final data in long distances. In order to achieve those goals, an appropriate signal processing system was designed and developed. This circuit consists of several stages, which are needed to increase the Signal to Noise Ratio (SNR) of the acoustic input signal and finally, create a suitable signal that can be digitized and further processed via a microcontroller. These stages, including preamplification, DC biasing, Analog-to-Digital Conversion (ADC) and a microcontroller unit, are illustrated in the block diagram of Figure 3.

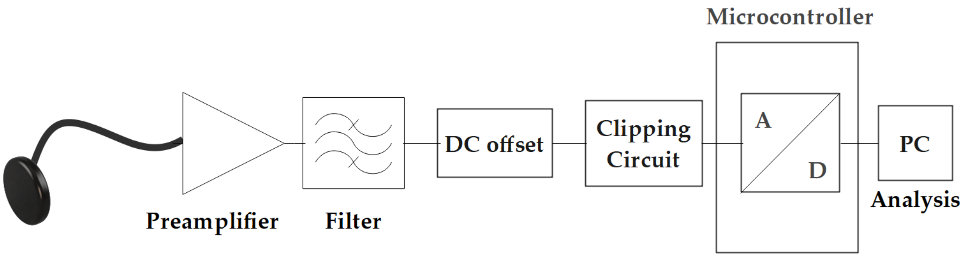


Figure 3. Block diagram of hydrophones electronics.

At the first stage of processing, the electrical analog signals, which are produced from the piezoelectric sensor, are subjected to amplification, in order to achieve better SNR [18]. The preamplification circuit, with high input impedance, increases the magnitude of the signal and at the same time reduces its noise. Low voltage and current noise are also critical characteristics of the operational amplifier that is used as the preamplifier for this purpose. At this stage of amplification, a gain factor of 3 was selected, as a tradeoff between high SNR and clipping of the signal.

The following stage includes an electronic circuit that adds a DC offset to the analog preamplified signal, which contains both a positive and a negative part. This process is necessary, as the signal's digitalization will then be held by a microcontroller that can only handle positive voltages. Thus, by adding a DC offset of half of the supply voltage of the microcontroller, the input signal is shifted to the positive part, preventing any damage to it. This stage is implemented by a simple voltage divider, consisting of two resistors having the appropriate values for the required voltage output value. Figure 4 is the measurement result that validates the expected performance of the above-mentioned stages, presenting the output signal after preamplification and DC biasing (yellow waveform), based on a sinusoidal input signal of 200 mV_{pp} (green waveform).

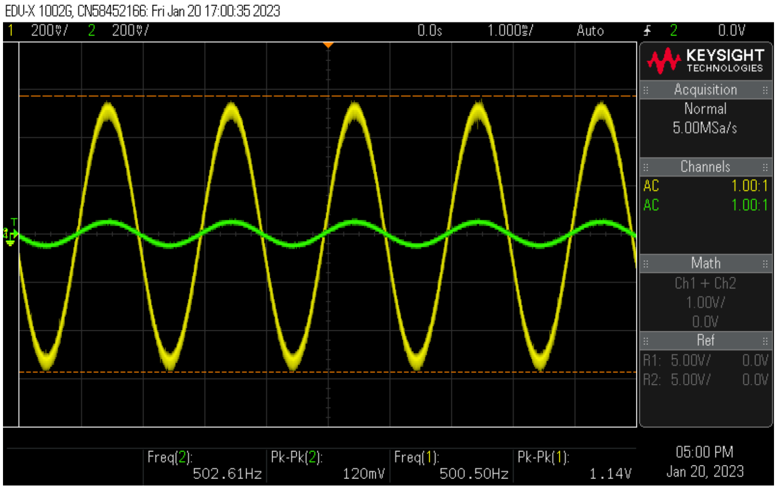


Figure 4. Measurement results of the output signal (blue waveform) after preamplification and DC biasing of the input signal (green waveform).

Another very significant process to which the signal is subjected before its digitalization, is the limitation of its amplitude, in order to prevent voltage spikes that may be generated due to high sound levels or collisions of the hydrophone on the sea bottom. As a result, a clipping protection stage was implemented prior to the ADC stage. In order to transmit the signal over long distances, as well as to further analyze it by a computer, the digitalization of the signal is required. For this purpose, there is a need of a fast and low power consumption microcontroller, which will be responsible for the Analog-to-Digital Conversion (ADC) of the signal.

2.4 OVERALL HYDROPHONE DEVICE

Given that the main purpose of a hydrophone is to operate on the field, the electronics enclosure must be at least weatherproof. For this purpose, an IP68 enclosure was used in order to house the developed PCB board (Figure 5). Moreover, the enclosure offers a USB cable for its communication and power supply. As a result, the overall device is compact and can be connected to a variety of equipment, such as data loggers, recording devices, or computers, using a cable interface. It must be noted that, at this stage of the device's development, it was not our intention to develop a waterproof electronics enclosure. Instead, the electronics can be kept near the data acquisition device (e.g., a laptop), while the hydrophone will be submerged in nearby waters an indicative distance of 15 m.

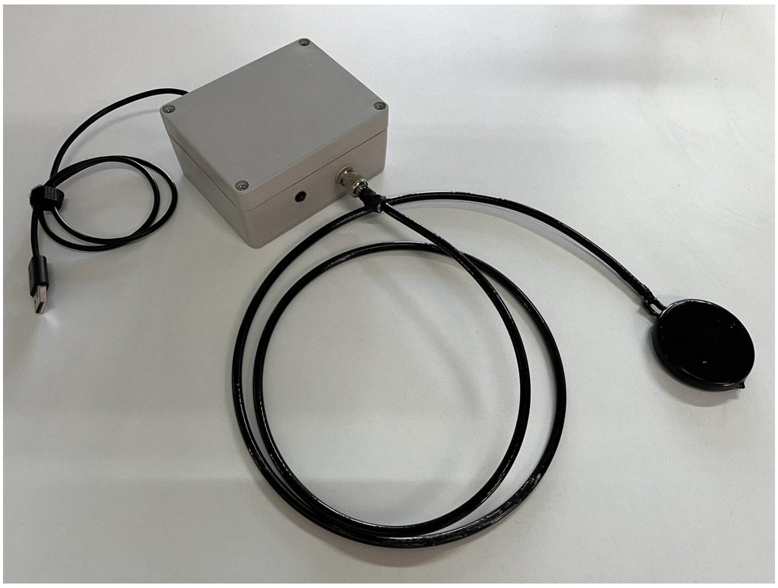
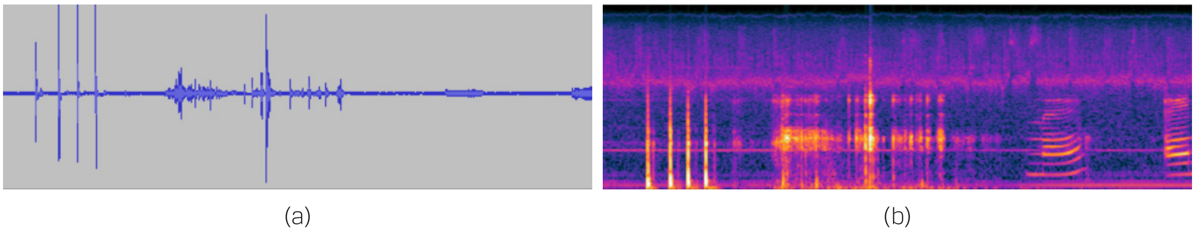


Figure 5. The final device, consisting of the waterproof sensor and the electronics enclosure.

2.5 DIGITAL SIGNAL PROCESSING

The developed device can function as an audio card with a connected audio input (i.e., the hydrophone). By using a typical audio software, the acquired signal can be recorded and further processed. Furthermore, the signal can be visualized as an audio waveform or a spectrogram. As a result, useful conclusions can be drawn about the recorded sounds and the audio sources that generate them. An example of the visualization of a recorded audio signal is shown in Figure 6. Figure 8a represents the waveform of the signal, while Figure 6b shows its spectrogram.



(a) (b)

Figure 6. Example of an audio signal recorded by the developed hydrophone device, visualized as (a) A waveform; (b) A spectrogram.

3. RESULTS

3.1 DIRECTIVITY AND RECEIVING SENSITIVITY

In order to mitigate the possibility of acoustic signal reflections caused by the tank walls, a porous insulator placed around the inside walls of the tank. Figure 7 illustrates the directivity of the developed hydrophones. It is quite obvious that hydrophones have omnidirectional response of approximately -20dB with deviation of ± 2 dB at 10 kHz for both horizontal and vertical axis. Finally, Figure 8 illustrates hydrophone's receiving sensitivity from 0.1 Hz to 10 kHz for both the commercial and the lab-developed hydrophones.

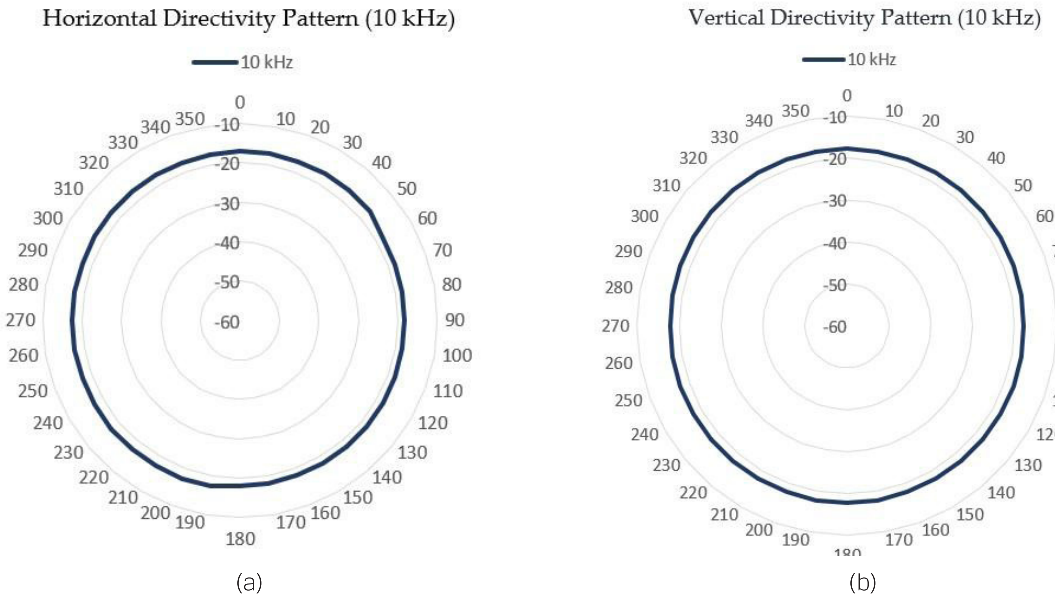


Figure 7. Hydrophone's: (a) horizontal; (b) vertical directivity pattern at 10 kHz.

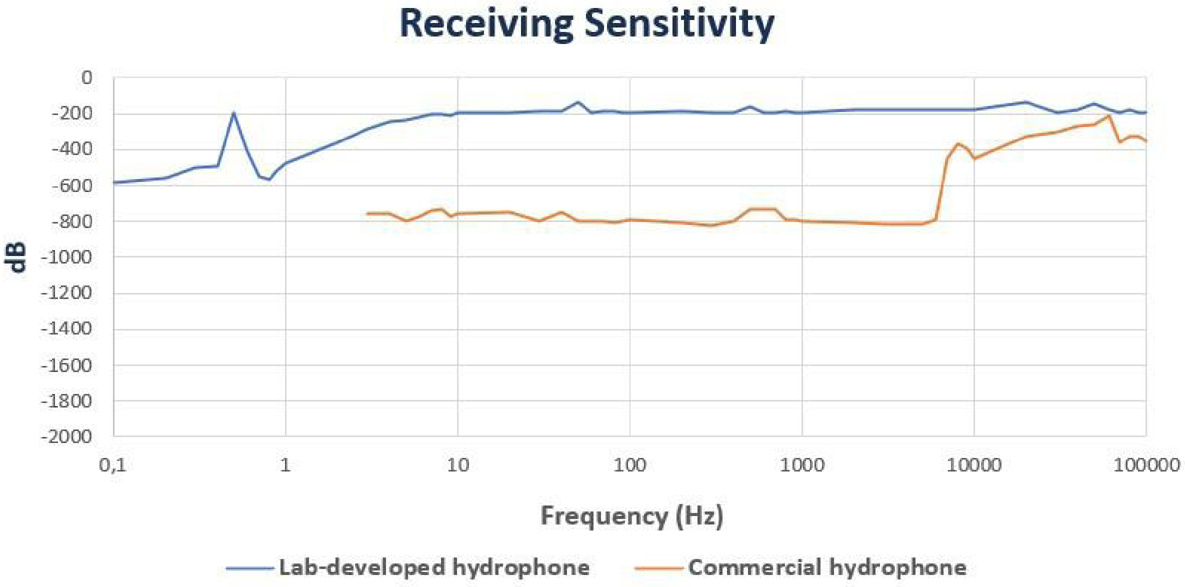


Figure 8. Hydrophone's receiving sensitivity for lab-developed (blue line) and the commercial (orange line) hydrophones.

4. DISCUSSION

The measurements which took place in the insulated tank, showed that the developed hydrophone is omnidirectional with an almost flat acoustic response at the wide usable acoustic range (Figure 8). More specifically, unlike the commercial hydrophone, the total lab-developed operating frequency range is from 0.1 Hz to 100 kHz.

As shown in Figure 3 the acoustic signal, imported from the hydrophone, passes through several stages, before it ends up to a personal computer. More specifically, the signal is subjected to amplification, ADC conversion, using a suitable microcontroller for this purpose. All the electronics are placed on a custom PCB and are enclosed in a weatherproof case. As a result, it has been designed a complete device for underwater acoustic signals, which can easily be used for measurements on the field.

The next step is to test the acoustic response and the sensitivity of the hydrophones in free-field conditions, namely in seawater to monitor their response. In order to ensure the stability of the sensing element while taking measurements, as well as the hydrophone's directivity, various support structures have already been designed, which include the use of one or two aluminum surfaces, placed parallel to the hydrophone. According to previous studies, the placement of metal plates offers better response at low frequencies, limitation of the harmonic components of the received audio signals, as well as mechanical stability to the hydrophone [4,19]. The mounts were 3D-printed, with a waterproof material, exhibiting high strength under various conditions. Using the arrangement with one aluminum plate (Figure 9b), the output of the received signal is expected to have better sound quality and less noise, compared to the arrangement with two aluminum plates (Figure 9a).

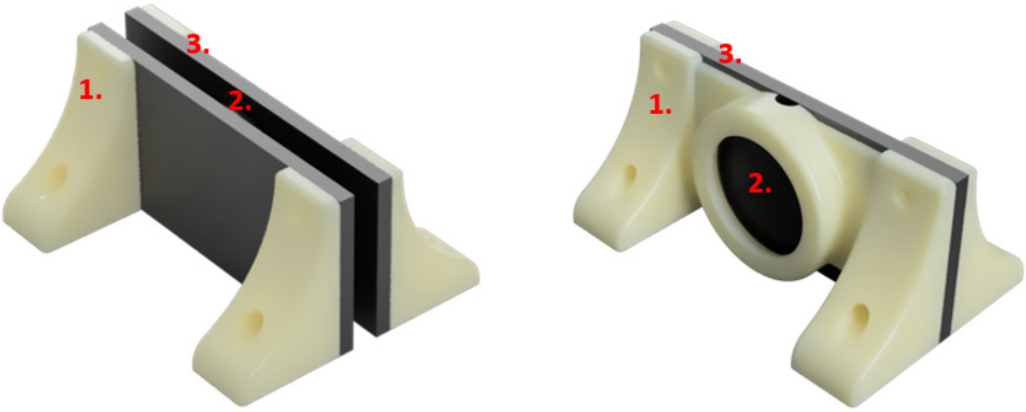


Figure 9. (a) Hydrophone's arrangement with one aluminum plate; (b) Hydrophone's arrangement with two aluminum plates, where (1) are the 3D-printed supports, (2) are the hydrophone location, and (3) are the aluminum plates.

5. CONCLUSIONS

In this study, the design and the development of an entire acoustic system that involved all the components (sensing element, packaging electronics, hardware and connection to signal processing application pipeline) using low-cost materials is thoroughly examined. The lab-developed hydrophone presents high sensitivity at a wide spectrum which ranges from 0.1 Hz to 100 kHz. Furthermore, an electronic circuit was designed and prototyped, to improve hydrophone's performance and digitize its output, in order to perform further signal analysis through a personal computer. More specifically, the circuit includes a stage of preamplification, a stage of DC biasing, a stage of Analog-to-Digital Conversion and a microcontroller, in order to receive an analog signal, digitize and analyze it, using specialized audio software. All these stages of acoustic signal process are placed on a PCB. Moreover, a weatherproof enclosure is used, to protect the designed electronic circuit during the on the field measurements. So, it has been designed a compact device, which can be connected to a personal computer and provide a lot of information about the underwater life taking as input acoustic signals.

REFERENCES

[1] Aronov, B.S. Nonuniform Piezoelectric Circular Plate Flexural Transducers with Underwater Applications. J. Acoust. Soc. Am. 2015, 138, 1570–1584, doi:10.1121/1.4928956.

[2] Butler, J.L.; Sherman, C.H. Transducers and Arrays for Underwater Sound; 2nd ed.; Springer International Publishing: Basel, Switzerland, 2016; ISBN 9783319390444.

[3] Marage, J.-P.; Mori, Y. Sonar and Underwater Acoustics; 1st ed.; Wiley-ISTE, 2013; ISBN 9781118600603.

[4] Saheban, H.; Kordrostami, Z. Fundamental Features, Design Considerations, and Various Structures: A Review. Sens. Sens. Actuators A Phys 2021, 329, doi:10.1016/j.sna.2021.112790.

[5] Hayman, G.; Robinson, S.P. Phase Calibration of Hydrophones by the Free-Field Reciprocity Method.; Acoustical Society of America, 2012.

[6] Cui, S.; Khoo, D.W.Y. Underwater Calibration of Hydrophones at Very Low Frequencies from 30 Hz to 2 KHz. J. Phys. Conf. Ser. 2018, 1065, 072015, doi:10.1088/1742-6596/1065/7/072015

[7] Koch, C. Amplitude and Phase Calibration of Hydrophones by Heterodyne and Time-Gated Time-Delay Spectrometry. IEEE Trans. Ultrason. Ferroelectr. Freq. Control 2003, 50, 344–348, doi:10.1109/tuffc.2003.1193629.

[8] Safari, A.; Akdogan, E.K. Piezoelectric and Acoustic Materials for Transducer Applications; Safari, A., Akdogan, E.K., Eds.; Springer: New York, NY, 2008; ISBN 9780387765402.

[9] Harris, G.R.; Gammell, P.M.; Lewin, P.A.; Radulescu, E.G. Interlaboratory Evaluation of Hydrophone Sensitivity Calibration from 0.1 to 2 MHz via Time Delay Spectrometry. Ultrasonics 2004, 42, 349–353, doi:10.1016/j.ultras.2003.12.008.

[10] Chen, H.; Zheng, Y.-J.; Hu, H.-P.; Fan, G.-F.; Lv, W.-Z. Analysis on Performance of an Infrasound Piezoelectric Hydrophone. In Proceedings of the 2016 Symposium on Piezoelectricity, Acoustic Waves, and Device Applications (SPAWDA); IEEE, 2016.

[11] Okada, N.; Takeuchi, S. Effect on High-Intensity Fields of a Tough Hydrophone with Hydrothermal PZT Thick-Film Vibrator and Titanium Front Layer. IEEE Trans. Ultrason. Ferroelectr. Freq. Control 2017, 64, 1120–1126, doi:10.1109/TUFFC.2017.2696052.

[12] Liu, J.-C.; Cheng, Y.-T.; Ho, S.-Y.; Hung, H.-S.; Chang, S.-H. Fabrication and Characterization of High-Sensitivity Underwater Acoustic Multimedia Communication Devices with Thick Composite PZT Films. J. Sens. 2017, 2017, 1–7, doi:10.1155/2017/7326919.

[13] Vasconcelos, D.; Nunes, N.J. A Low-Cost Multi-Purpose IoT Sensor for Biologging and Soundscape Activities. Sensors (Basel) 2022, 22, 7100, doi:10.3390/s22197100.

[14] De Marco, R.; Di Nardo, F.; Lucchetti, A.; Virgili, M.; Petetta, A.; Veli, D.L.; Screpanti, L.; Bartolucci, V.; Scaradozzi, D. A Low-Cost Approach in Acoustic Monitoring of Dolphin Presence. In Proceedings of the 2022 IEEE International Workshop on Metrology for the Sea; Learning to Measure Sea Health Parameters (MetroSea); IEEE, 2022.

[15] Yang, D.; Zhao, J. Acoustic Wake-up Technology for Microsystems: A Review. Micromachines (Basel) 2023, 14, 129, doi:10.3390/mi14010129.

[16] Roh, T.; Yeo, H.G.; Joh, C.; Roh, Y.; Kim, K.; Seo, H.-S.; Choi, H. Fabrication and Underwater Testing of a Vector Hydrophone Comprising a Triaxial Piezoelectric Accelerometer and Spherical Hydrophone. Sensors (Basel) 2022, 22, 9796, doi:10.3390/s22249796.

[17] Anthoni, J. The Chemical Composition of Seawater. Magnesium 2006, 2701.

[18] Manoj, G.; Sreedevi, K.; Gopal, V. Significance of a Low Noise Preamplifier and Filter Stage for Under Water Imaging Applications. Procedia Comput. Sci., vol. 93, pp. 585–593, 2016, doi: 10.1016/j.procs.2016.07.241.

[19] Li, D.; Wu, M.; Oyang, P.; Xu, X. Cymbal Piezoelectric Composite Underwater Acoustic Transducer. Ultrasonics 2006, 44 Suppl 1, e685-7, doi:10.1016/j.ultras.2006.05.127.

GAS SENSORS EQUIPPED WITH BLACK METAL ACTIVE LAYERS

Jan Kejzlar[1].

Abstract

This essay is focused on study, fabrication and application of highly sensitive gas sensors working as chemiresistors, equipped with black metal active layers. The term "black metal" denotes a specific form of metallic material with extremely high porosity, gas sorption capacity and catalytic activity. Sensors equipped with such layers could be used as early warning systems for civil population, secondary prevention of terrorist attacks or as modular parts of mobile devices for field operations. The potential for these sensor devices is also in the industry, cities or households to monitor the quality of air, leaks of dangerous substances or general presence of various gasses. The black metal layers can be also decorated with various substances, such as MXenes to further improve their sensing capabilities. The future research should be focused on finding and improving the deposition techniques to enhance mechanical, physical, and chemical properties of such layers for specific purposes.

Keywords

Gas detection, Black metals, Security, Nanostructured materials, Chemiresistors.

1. INTRODUCTION

Gas sensing devices are nowadays abundantly used in various industries, it is therefore essential and highly relevant to search for improvements of such devices. The way proposed in this essay, is to use a highly sensitive active layer made of a nanostructured black metal (BM). Key features of the BMs are their high surface to volume ratio, high sorption capacity and catalytic activity. These attributes make the BMs ideal candidates for usage in the gas sensing apparatus.

Over the years, numerous methods for BM preparation were developed, including (but not limited to) the chemical dealloying, laser etching, magnetron sputtering or thermal evaporation. This essay offers a short glimpse on these technologies, with an extra focus on the magnetron sputtering and thermal evaporation.

In order to achieve the desired response on the measured gas analyte, the BM layer has to be deposited on a suitable substrate. One can either observe the alteration of the resonant frequency on the quartz crystal microbalance (QCM) sensor, which depends on the weight of the adsorbed molecules on the surface of the active layer. The other option is to use the BM as a sensitive layer in the chemiresistor, which implies a device that changes its electrical resistance or impedance in dependence on a certain chemical stimulus i.e., the presence of a certain chemical in the analysed environment. This essay focuses on the latter.

2. CURRENT STATE-OF-THE-ART

2.1. BLACK METALS

Metal films, with a highly nanostructured surface morphology, are called black metals or metal blacks due to their optical properties. The surface of such films is densely populated by various nanostructures, resulting in a cauliflower-like morphology, as seen in Figure 1. Due to this factor, the optical absorbance of these layers in visible region can be well above 90% [1]. So far, BMs found application in the solar collectors or heat transfer devices [2],

[1] University of Chemistry and Technology, Prague, Czech Republic kejzlarj@vscht.cz

optical sensing and imaging devices [3] or solar cells [4]. However, the application of the BMs as the active layers for the chemiresistors is in pioneering stage, with high potencial for the future.

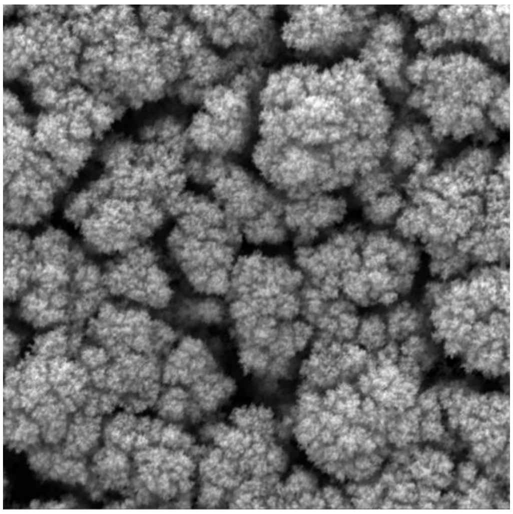


Figure 1: Surface morphology of black gold film.

In the terms of the electrical properties, the BMs behave as metals. Their electric resistivity increases with temperature (the same trend, but different magnitude when compared with a bulk metal).

2.2. BLACK METAL PREPARATION

To obtain the nanostructured surface of the BM, the source material must be deposited or leached in such a manner that it forms a layer with a high surface to volume ratio. This structure can be obtained via the physical vapor deposition techniques, such as the thermal evaporation or magnetron sputtering. The altennative methods consist of the laser nanostructuring, electrochemical deposition or chemical etching.

During thermal evaporation, the source material is evaporated from the tungsten or molybdenum boat and condensed on the substrate in a vacuum chamber (see Figure 2). To obtain a BM layer, inert atmosphere of the argon, nitrogen or other gas is introduced into the chamber. The evaporated metal particles then collide with the inert, loosing their kinetic energy to such a degree, that they cannot migrate on the substrate surface and remain fixed in the arbitrary positions, resulting in the nanostructured material morphology.

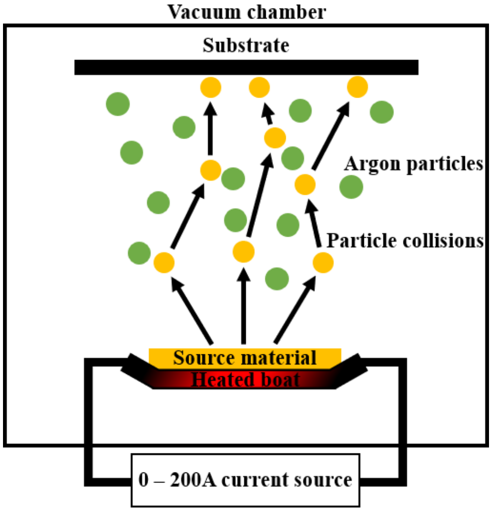


Figure 2: Scheme of the thermal evaporation technique.

The magnetron sputtering is a technique, where the source material is bombarded by the argon ions, tearing the atoms and clusters of the source material, which then rests upon the substrate. By introducing a small percentage (~6%) of nitrogen into the working atmosphere, the growth of the film on the substrate can be altered to form a BM layer [5].

The laser nanostructuring is operating with highly focused femtosecond laser pulses to engrave on the surface, which leads to alterations of optical properties of the target material [6]. The main advantages offered by this method is the option to process a wide variety of materials, including metals, glasses or semiconductors. The beam can be also focused on the surface, thus producing a variety of complex structures.

Another group of techniques consist of the chemical and electrochemical dealloying. The chemical dealloying is a common corrosion process during which, the less noble metal is dissolved from an alloy, leaving a nanoporous sponge-like structure of the second component [7]. The electrochemical dealloying differs from the chemical one by applying an external electrochemical potential in the acidic electrolyte. A multi-step method, where the Ag-Au alloy was first etched in a 1:2 diluted acid solution (30ml HNO3 and 60ml of H2O) and then in pure 70% HNO3 solution was reported to be very successful in preparation of nanoporous gold [8].

2.3. POTENTIAL OF BLACK METALS IN GAS SENSING

The BMs in fact possess a high potential for the chemiresistive active layers due to the number of physical and chemical properties. Firstly, the Gibbs energy of the BM is much higher than that of a bulk metal, this promotes the interaction between the BM layer and the gaseous analyte. The surface of the BM layer also showcases a high catalytic activity (it decomposes larger molecules into easily detectable reactive fragments). In contrast to oxides, commonly used in the chemiresistors, the BMs can readily form complexes with Lewis's bases (CO, HCN) even at the laboratory temperature, such a reaction is accompanied by the charge transfer, affecting the electrophysical properties. Lastly, the surface of the BM can be easily modified by suitable organic or inorganic substances (MXenes, Thiols) to further improve the selectivity. An example of a sensoric response to a gas analyte can be seen in Figure 3.

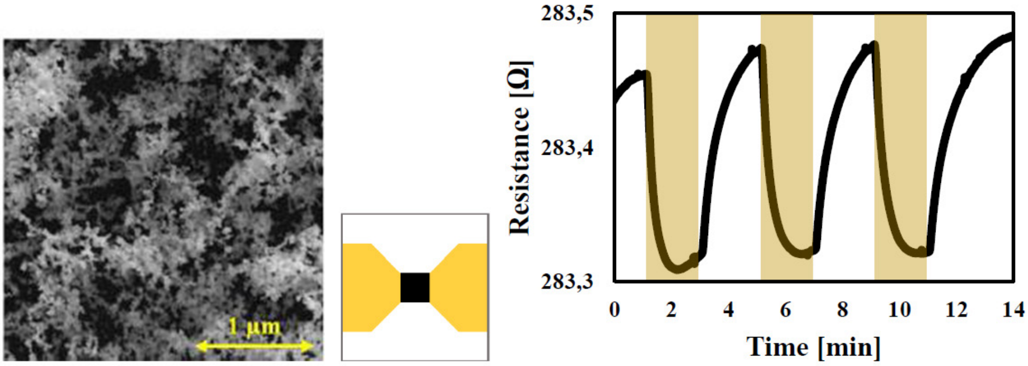


Figure 3: Black antimony nanostructure (left); chemiresistor scheme with gold electrodes and black Sb active layer (middle); response of this sensor to 10 ppm of nitrogen dioxide – yellow stripes, reference gas was synthetic air – white stripes (right)

A unique property of chemiresistors with BMs is to utilize so-called skin effect. When measuring the sensor response by an AC signal at sufficiently high frequencies (~10^9 Hz), then the current density in the metallic sensitive layer stays localized near its surface in the so-called "skin depth" δ. The skin depth δ (m) can be obtained according to the formula:

$$\delta = \frac{1}{\sqrt{f\pi\mu\sigma}}$$

Where f (Hz) denotes signal frequency, μ (H*m^{-1}) magnetic permeability of the metal and σ (S*m^{-1}) its specific conductivity. A particular interesting situation occurs, when ferromagnetic metals with high μ values are employed. Thus, e.g., cobalt provides δ = 90 nm and nickel δ = 170 nm at f = 3GHz. As a consequence, in such mode of measurement, the depth from which sensing information is collected can be easily tuned by setting the signal frequency. This property of the BMs is unique, unattainable by the commonly used materials used as chemiresistive active layers (oxides, conductive polymers).

3. POTENTIAL IN INDUSTRY AND DEFENCE

3.1. GENERAL CONCEPT OF THE BLACK METAL UTILIZATION

The main potential of the black metals lies in their ability to significantly enhance the sensing properties of the gas detecting devices. For example, study by Hieda et. al. from 2017 proposed a sensor based on porous single-crystalline ZnO nanosheets modified by gold nanoparticles. The results showed that the detection limit is 10 ppb of trimethylamine, which is important for monitoring the quality of foods in storage or during transportation [9]. This concept of an augmentation could be used in a number of applications, some of them being discussed in the following chapters. Another advantage is the possibility to manufacture small detection devices, resulting in a cheap, modular, and replaceable equipment.

3.2. INDUSTRIAL APPLICATIONS

Majority of industrial processes and applications need to monitor some sort of gaseous analyte. Among others, various products, intermediates and biproducts need to be monitored during the production. If we take a closer look, the gas leaks costs billions of dollars and hundreds of lives. For example gas pipeline incidents from 2010 to 2021 cost 3 859 millions of dollars and the explosions connected cost 122 human lives and caused another 602 injuries [10]. The gas sensors could be used to prevent or at least drastically reduce such incidents. Other utilization of BM gas sensors could be the monitoring of the quality of air in the working environment or public places, such as a city infrastructure.

3.3. DEFENCE SYSTEMS APPLICATIONS

In the recent years, terrorist acts are a significant security problem. According to the National Consortium for the Study of Terrorism and Responses to Terrorism (START), the number of terrorist attacks in the USA increased from 10 in 2011 to 65 in 2017 [11]. One of the most frequently used forms of terrorist attacks is the usage of explosives in order to harm civil population (bombing and suicidal bombing attacks, plane bombing, etc.). In these cases, the main victims are innocent people not participating in the conflict. Direct vapor detection of many explosives is a difficult task, as their vapor pressure is extremely low. However, most of the used explosives bought on the black market are made by licensed manufacturers that use volatile taggants that can be detected. Well organised terrorist groups are also able to acquire or manufacture and consequently use chemical warfare agents such as Sarin (Tokyo metro Sarin attack in 1995). These agents are classified into the blister, nerve, blood and pulmonary agents. Although known for more than a century, these agents still pose a severe threat, as they are relatively easy to manufacture and have a devastating effect.

The detection of volatile explosive taggants and chemical warfare agents is therefore critical to protect the civil population across the globe. Gas detectors enhanced by BM active layer could be used for these purposes and serve in the early warning and prevention systems. Other application could be the usage of drones equipped with such detectors for field operations in a hard or hazardous conditions, which would be dangerous for human operators.

3.4. OTHER APPLICATIONS

Gas sensing systems are developed for current applications such as the Internet of Things (IoT), mobile and wearable devices. The wider – social – consequences of the research and development in sensor area can be seen in the detection of harmful gasses, environmental monitoring, and also protection of the civil population from health risks. A high degree of miniaturization, simultaneously with maintaining relevant parameters and low cost of the produced sensors is requested in those applications. Therefore, high sensitivity, selectivity, low limit of detection in the range of ppb without pre-concentration and long term stability are essential requirements for modern gas sensors. Currently, they are only partially accomplished in today's commercial detectors (Figaro microhot-plate MEMS-based sensor TGS8100) for personal safety measurement of gases such as CO, NH4, NOX, Co2. One alternative is to use the BM based sensing materials.

4. FUTURE DEVELOPMENT

As for the surface decoration of BMs, it is advantageous to arrange the active layer of chemiresistors so that the continuous bottom layer made of the BM (acting predominantly as a transducer) is surface decorated by MXenes (acting predominantly as a receptor). In such an arrangement (during the measurement of the sensor response), that the dc-current or ac-current at lower frequencies will flow preferably in the BM layer (although the MXenes also have metal- type conductivity that reaches a maximum of 103 S.m-1 [12], but this is about three orders of magnitude less than that of the BM). However, when measured in the GHz frequency range, the skin effect will ensure current flow through the BM surface or the MXene, so the current signal will be collected from different parts of the active layer. In addition, when interacting with certain analytes, the MXenes are known to switch their conductivity from metal to semiconductor type [13]. Under such circumstances, a semiconductor-metal heterojunction can be formed on the surface of the layer [14]. Because the positions of the Fermi levels in both materials are different, the electron density of MXene increases, thereby stimulating atmospheric oxygen chemisorption and the spill-over effect [15].

5. CONCLUSION

In conclusion, although some pilot experiments were already carried out, the BMs still possess a huge potential in the field of gas sensing. Gas detectors equipped with the BM active layers could find their use in the fields of defence, civil protection or environmental monitoring. As we can see, due to the numerous accidents, terrorist attacks or in general need of monitoring of the gaseous analytes, gas sensor development is very important for the safety, economically and from a defensive point of view.

ACKNOWLEDGEMENTS

I would like to thank to my supervisor prof. Dr. Ing. Martin Vrňata for his consultations and time.

REFERENCES

[1] W. Becker, R. Fettig, A. Gaymann, and W. Ruppel, "Black gold deposits as absorbers for far infrared radiation," Phys. Status Solidi Basic Res., vol. 194, no. 1, pp. 241–255, 1996, doi: 10.1002/pssb.2221940123.

[2] L. Harris and P. Fowler, "Absorptance of Gold in the Far Infrared*," J. Opt. Soc. Am., vol. 51, no. 2, p. 164, 1961, doi: 10.1364/josa.51.000164.

[3] A. B. Christiansen et al., "Black metal thin films by deposition on dielectric antireflective moth-eye nanostructures," Sci. Rep., vol. 5, no. June, pp. 1–9, 2015, doi: 10.1038/srep10563.

[4] D. Panjwani et al., "Metal-black scattering centers to enhance light harvesting by thin- film solar cells," Energy Harvest. Storage Mater. Devices, Appl. II, vol. 8035, p. 80350N, 2011, doi: 10.1117/12.883467.

[5] J. More-Chevalier et al., "Fabrication of black aluminium thin films by magnetron sputtering," RSC Adv., vol. 10, no. 35, pp. 20765–20771, 2020, doi: 10.1039/d0ra00866d.

[6] A. Y. Vorobyev and C. Guo, "Colorizing metals with femtosecond laser pulses," Appl. Phys. Lett., vol. 92, no. 4, pp. 1–4, 2008, doi: 10.1063/1.2834902.

[7] R. Liquid, J. Erlebacher, M. J. Aziz, A. Karma, and N. Dimitrov, "Evolution of nanoporosity in dealloying," vol. 410, no. March, pp. 5–8, 2001, doi: 10.1103/PhysRevB.50.8016.

[8] Y. Sun and T. J. Balk, "A multi-step dealloying method to produce nanoporous gold with no volume change and minimal cracking," Scr. Mater., vol. 58, no. 9, pp. 727–730, 2008, doi: 10.1016/j.scriptamat.2007.12.008.

[9] F. Meng, H. Zheng, Y. Sun, M. Li, and J. Liu, "Trimethylamine sensors based on au- modified hierarchical porous single-crystalline ZnO nanosheets," Sensors (Switzerland), vol. 17, no. 7, 2017, doi: 10.3390/s17071478.

[10] T. Dutzik, A. Scarr, and M. Casale, "Methane Gas Leaks: Frequent leaks are resulting in death, injury and other damage to our health and environment." [Online]. Available: https://publicinterestnetwork.org/wp-content/uploads/2022/08/Methane-Gas-Leaks- 2022.pdf.

[11] E. Miller and M. Jensen, "American Deaths in Terrorist Attacks, 1995 - 2017," no. 2012, pp. 1–2, 2018, [Online]. Available: https://www.start.umd.edu/pubs/START_AmericanTerrorismDeaths_FactSheet_Sept201 8.pdf.

[12] K. Hantanasirisakul and Y. Gogotsi, "Electronic and Optical Properties of 2D Transition Metal Carbides and Nitrides (MXenes)," Adv. Mater., vol. 30, no. 52, pp. 1–30, 2018, doi: 10.1002/adma.201804779.

[13] K. Deshmukh, T. Kovářík, and S. K. Khadheer Pasha, "State of the art recent progress in two dimensional MXenes based gas sensors and biosensors: A comprehensive review," Coord. Chem. Rev., vol. 424, 2020, doi: 10.1016/j.ccr.2020.213514.

[14] T. He et al., "MXene/SnO2 heterojunction based chemical gas sensors," Sensors Actuators, B Chem., vol. 329, p. 129275, 2021, doi: 10.1016/j.snb.2020.129275.

[15] J. Wen et al., "MXene-derived TiO2 nanosheets decorated with Ag nanoparticles for highly sensitive detection of ammonia at room temperature," J. Mater. Sci. Technol., vol. 114, pp. 233–239, 2022, doi: 10.1016/j.jmst.2021.12.005.

AUTHOR

Jan Kejzlar was born in Trutnov in 1996. He got his master's degree in 2020 at the Institute of Chemistry and Technology, Prague. Now, he is a PhD student at the Sensor Group of the Department of Physics and Measurements at the University of Chemistry and Technology, Prague. His current research is focused on preparation of the black metal layers using thermal evaporation and magnetron sputtering.

IMPROVED DETECTION OF HYPERSONIC THREATS WITH RADAR USING IRREGULAR WAVEFORMS AND ADVANCED PROCESSING

Pepijn Cox[1], Keith Klein[1], Mario Coutiño[1], and Laura Anitori[1].

Abstract

Hypersonic weapons can pose a significant threat to the international security, as the characteristics in terms of speed, cruise altitude, and manoeuvrability differ significantly from other threats. This implies that the engagement timelines become extremely short and, hence, the detection, tracking, classification, and identification should be accomplished at large distances. To fulfil these tasks, current radar sensors will be pushed to or beyond their current limits. A potential solution to overcome certain limitations of modern radar systems is by using novel waveforms and advanced signal processing. Hence, the goal of this work is to demonstrate the potential of irregular waveforms and advanced processing for the detection of hypersonic threats. It is shown that their combination can significantly increase the detection performance and the measurement accuracy compared to multiple, medium pulse repetition frequency waveforms with linear signal processing.

Keywords

Advanced radar signal processing, Irregular waveforms, Hypersonic threats, Radar systems.

1. INTRODUCTION

The introduction of hypersonic weapons to the battlefield will be disruptive. High velocities, manoeuvrability, and relatively low cruising altitudes of these threats makes effective engagement difficult, as the first generation hypersonic missiles have unfortunately shown in the Ukraine [1]. The threat characteristics of the hypersonic weapons are significantly different than that of ballistic and cruise missiles and novel solutions are needed for successful interception [2], [3]. The complexity of the problem suggests that a sensor network could be an effective solution for a successful kill-chain.

That said, the required performance for the tasks assigned to each sensor within such a network might be pushed to or beyond the current limits. The engagement timelines become extremely short due to the hypersonic speed, cruise altitude, and threats' manoeuvrability requiring that the detection, tracking, classification, and identification are accomplished at large distances to have sufficient time for target engagement, where several tasks are primarily fulfilled by radar systems.

Detection by radar systems depends on the system parameters and on the radar cross section (RCS) of the target, where a small value implies that it is more difficulty to observe. Currently, there are several studies in e.g., EDA and NATO to understand the phenomenology of hypersonic threats [3], [4]. Plasma effects surrounding the hypersonic vehicle makes the to-be-expected RCS value highly uncertain and it is possibly subjected to significant variations.

Modern surveillance radar systems employ multiple, medium pulse repetition frequency (PRF) type of waveforms with linear signal processing on receive for the detection of typical current targets. The waveforms commonly consist of several bursts, each burst containing multiple identical pulses at a constant carrier frequency and PRF. To obtain unambiguous estimates of the target's range and velocity from the measurements, the concept of staggered PRF waveforms is often used. This concept results in longer transmission times and processing losses,

[1] Radar Technology Department, TNO, The Hague, The Netherlands {pepijn.cox;keith.klein;mario.coutinominguez;laura.anitoro}@tno.nl

but the signal processing is rather straightforward and suited for real-time implementation. For the surveillance of hypersonic threats, the staggered PRF waveforms and linear processing are pushed to their practical limits [5] in terms of detection performance and in terms of unambiguously estimating both the range and the radial velocity parameters of the target.

To summarize, the hypersonic threats pose challenges to individual radar systems in a network as: 1) the threat needs to be detected at a large range leading to a low signal-to-noise-ratio scenario; and 2) the staggered PRF waveforms with linear processing experience practical limitations leading to significant detection performance degradation.

Recent developments of commercial high performance computing using graphical processing units increases the processing capabilities far beyond the requirements of linear signal processing used in many radar systems. It potentially allows for the use of waveforms consisting of irregular intervals and/or irregular modulations combined with advanced, and possibly non-linear and iterative, signal processing techniques. This combination will [6], [7]: a) not experience ambiguities in the range and the radial velocity measurements, b) significantly decrease the processing losses currently experienced by linear processing, c) increase the accuracy of the range and velocity measurements, and d) decrease the susceptibility against deceptive electronic counter measures. Figure 1 provides an artist's impression of naval radar employing irregular waveforms and advanced processing using high performance computing. The potential of these novel concepts for radar is currently also explored within a DARPA program [8].

The goal of this work is to demonstrate the potential of irregular waveforms and advanced processing for the detection of hypersonic threats. In particular, it shows that the combination of irregular waveforms and advanced processing offers a potential solution for unambiguous range and velocity measurements while simultaneously increasing the detection range. In addition, this work also discusses our developments in 1) decreasing the computational load of the proposed advanced algorithms and 2) effective suppression of clutter when using irregular waveforms.

The paper is organized as follows. Irregular waveforms and advanced processing concepts for radar is given in Section 2. In Section 3, the performance of this solution for the hypersonic threat detection is given. The usage of irregular waveforms and advanced processing in the civil domain is briefly discussed in Section 4 followed by the conclusions in Section 5.

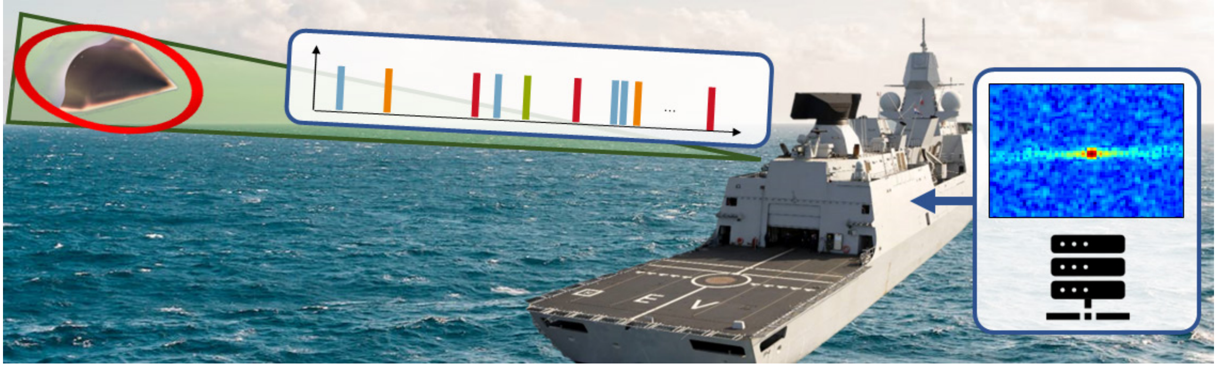


Figure 1. Artist's impression of naval radar employing irregular waveforms and advanced processing against hypersonic threats.

2. IRREGULAR PULSED WAVEFORMS AND ADVANCED PROCESSING

The emerging threat of hypersonic weapons imposes the need to expand the maximum detection range and the capabilities of unambiguously measuring the targets' ranges and velocities. To understand the limitations of systems employing staggered PRF waveforms with linear processing, we will discuss them briefly. Staggered PRF waveforms consist of a number of bursts where the i-th burst contains multiple identical pulses with a constant PRF_i and a constant carrier frequency f_i. The regularity in each burst leads to ambiguities in the range and the velocity measurements of the target. As the required range and velocity spans far exceed the requirements for surveillance of hypersonic threats, multiple bursts at different PRFs and carrier frequencies are transmitted and processed, with varying unambiguous ranges and velocities, see blue and orange areas in Figure 2.(left). A target appears for each burst at a different location, see blue crosses and orange plusses. Unfolding the measurements of each burst beyond this ambiguous domain and then overlaying the measurements of the different bursts will reveal the true location of the target, see green circle. In practice, the unfolding capabilities are limited [5], e.g., due to noise, blind ranges, and clutter filtering, which significantly decreases the detection performance.

Introducing irregularities in the pulse interval and/or pulse modulation is a way to resolve the range and the velocity ambiguities [7]. Absence of ambiguities removes the need for multiple incoherent bursts and the transmission time could be used for a single coherent waveform that significantly increases the detection performance[2]. On the other hand, processing irregular waveforms requires 1) advanced match filtering schemes to produce a high quality range and velocity image without significant losses and 2) the target detection requires iterative optimization techniques to handle the higher sidelobe levels of irregular waveforms. With increased sidelobes, strong targets can mask weak targets. For example, an airliner or sea clutter in the beam might mask a hypersonic target. To mitigate both issue, advanced processing plays a crucial role.

In this section, we highlight our recent developments [7], [9]-[14] in the design and processing of irregular waveforms, show how the extra degrees of freedom can be exploited, and how clutter can be supressed in an efficient way. In this section, we focus our discussion on irregular pulse intervals, but the techniques can also be extended to waveforms with irregular pulse modulation.

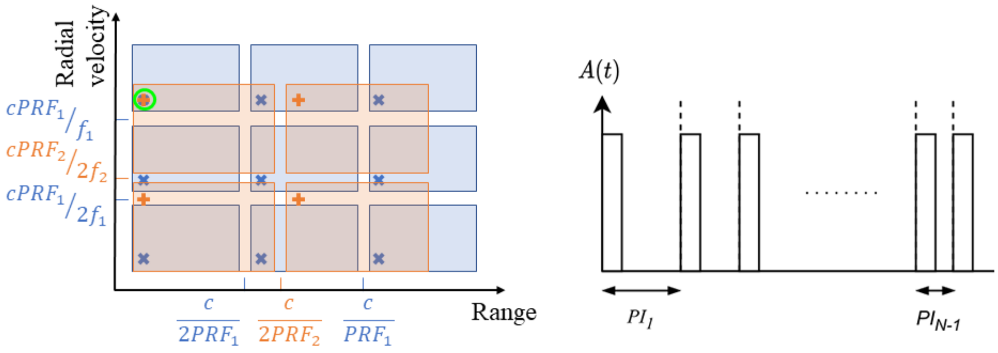


Figure 2. Illustration of the unfolding of a staggered waveform employing two bursts (left) and (right) an illustration of amplitude over time of an irregular pulse interval waveform.

2.1. WAVEFORM WITH IRREGULAR INTERVALS

To suppress periodic ambiguities in both range and velocity, irregularity can be introduced in the *pulse interval* (PI), e.g., by selecting the pulse interval of sequential transmitted pulses randomly on a uniform interval between a minimum and maximum value, see Figure 2.(right). In Figure 3, two ambiguity functions are shown for a) a *linear frequency modulated* (LFM) waveform with a regular PRF of 2 kHz at 1.2 GHz, and b) an LFM waveform with random PIs. Clearly, in Figure 3.(left), the range ambiguities at multiples of 75 km and the velocity ambiguities at multiples of 250 m/s are visible for the regular PRF waveform as peaks with almost equal amplitude to the main peak in the origin. The sidelobes, i.e., contributions in regions outside the main peak, are significantly lower for the regular PRF waveform compared to the irregular PI waveform, in both the range and radial velocity domain. However, removing the periodic ambiguities of the regular PRF waveform by using random PI waveforms come at the cost of increased sidelobes.

The ambiguity function represents the signal contribution of a single object at zero range and with zero radial

[2] The detection performance will increase under the assumption that the target remains coherent during the coherent integration time.

velocity. A complex radar scene is a superposition of amplitude scaled ambiguity functions of all targets and clutter, where the peak at (0,0) is moved to the range and velocity of the targets and clutter. Detecting these peaks allows to find objects in the scene. However, the strong sidelobes of slow moving clutter nearby can mask a fast moving hypersonic far away.

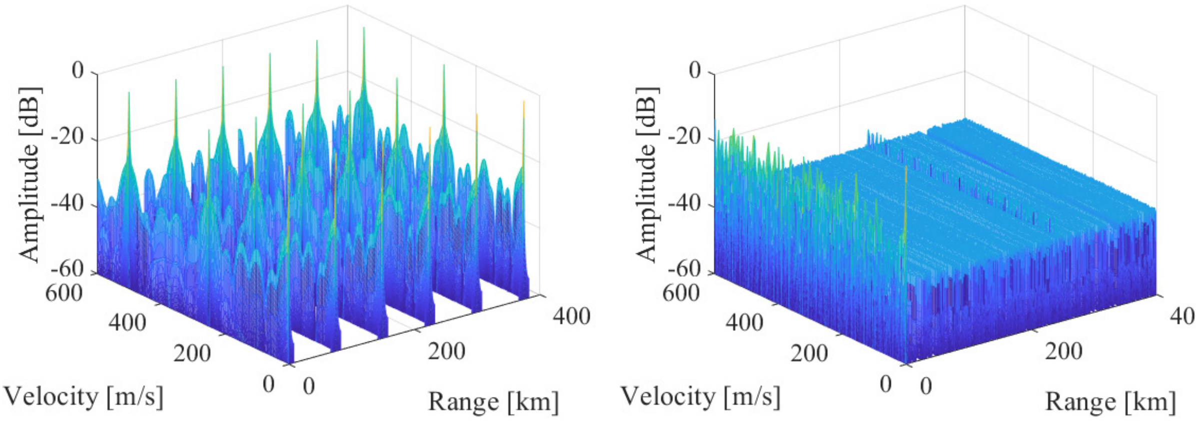


Figure 3. Ambiguity function of (left) a regular LFM waveform with PRF of 2 kHz at 1.2 GHz and (right) LFM waveform with random PIs on [0.25, 0.75] ms interval.

The sidelobes of the waveform can be modified and lowered in particular regions by optimizing the PI for particular scenarios. For example, lowering sidelobes of a clutter in the range-velocity region where the hypersonic target should be initially detected. See [9]-[11] for our current developments in waveform optimization.

2.3. CLUTTER SUPPRESSION

The detection of hypersonic threats at a large distance by radar systems close to the earth's surface implies small grazing angles, i.e., observations close to the horizon. This will introduce strong surface clutter into the observation. However, efficient mitigation of clutter for irregular waveforms is an open topic in the literature.

To mitigate the clutter in the received signal for irregular waveforms, we propose a modified filtering approach. Similar to standard *moving target indication* (MTI), our irregular MTI method exploits the fact that most clutter is found at close range and has a small velocity component [12]. When the irregular waveform has pulses with equivalent modulation, a simple and computationally efficient clutter filter can be implemented, see [12] for the details. The effectiveness of our irregular MTI method is highlighted in the next section.

The irregular MTI clutter filter is inadequate for filtering of waveforms with irregular modulation. We recently introduced a clutter filtering technique at a slight increased computational cost [13] to handle waveforms with both irregular pulse intervals and irregular modulation.

2.4. TARGET ESTIMATION WITH IRREGULAR WAVEFORMS

Irregular waveforms require advanced processing to 1) avoid large matched filtering losses due to the Doppler sensitivity of the waveform and 2) to handle the high sidelobe levels.

To generate an image of the scene similar to Figure 3 used for target detection, matched filtering (MF) is applied. Linear processing usually employs a *one dimensional* (1D) range MF and a separate 1D Doppler filter bank under the assumption that range and velocity processing can be performed independently. However, for irregular waveforms, independent processing leads to significant MF losses. To mitigate the matched filtering losses, in this paper, a *two dimensional* (2D) MF is applied, where a 2D MF accounts for all velocity shifts of interest for each pulse delay [14]. However, the 2D MF significantly increases the computational load compared to independent linear 1D processing.

Recently, we proposed an approximate 2D MF based on subpulse processing [12] that reduces the computational overhead and that can be efficiently computed by hardware accelerated FFTs.

To mitigate the high sidelobe levels of irregular waveforms, iterative processing techniques can be applied. As the radar only detects a couple of objects in the scene, the solution to our detection problem is sparse and, therefore, sparse optimization is applied in this paper. Many solvers exist to solve a sparse optimization problem, e.g., see [15], in our example the non-linear, iterative *orthogonal matching pursuit* (OMP) [14] is applied in Section 3.

3. SIMULATION STUDY OF THE HYPERSONIC THREAT DETECTION

In this section, the performance of the proposed irregular waveform and advanced, iterative 2D signal processing is compared to that of a typical staggered, medium PRF waveform with linear 1D processing for the detection of a hypersonic threat.

3.1. HYPERSONIC SURVEILLANCE SCENARIO DESCRIPTION

We consider the case of a single hypersonic threat modelled with a Swerling case I fluctuation model. The radial velocity can range between Mach 2 and Mach 18 and the threat is placed at a range between 300 km and 700 km from the radar system. The simulation includes sea surface clutter with sea state 3 modelled by the NRL model [16]. The clutter horizon is 12 km and the velocity spectrum is taken as Gaussian with 0.72 m/s standard deviation. For the sea clutter generation, it is assumed that the radar beam is fixed at an elevation of 3°. The target range and velocity are uniformly drawn from the above given brackets and only one target is present in every Monte Carlo run. For every simulation of the 3000 Monte Carlo runs, a new realization of the thermal noise, of the clutter, and of the target is generated on which the staggered PRF waveform with 1D processing and the irregular PI waveform with 2D processing are evaluated.

The staggered medium-PRF waveform consists of four bursts where the carrier frequency, number of pulses, and PRF are changed per burst. The pairs are chosen (1.23 GHz, 13, 1600 Hz), (1.20 GHz, 15, 1800 Hz), (1.18 GHz, 17, 2000 Hz), (1.21 GHz, 19, 2300 Hz), respectively. All pulses have an LFM modulation with a pulse length of 50 μs. For processing, a three-pulse MTI filter is used to mitigate clutter, a Hamming window for pulse compression is applied and for Doppler filtering a Hanning window is used. For the detector, the individual bursts are processed with the cell-averaging constant false alarm detector and the individual burst detections are then combined using an 2-out-of-4 detector.

The irregular waveform consists of irregular PIs with equal modulation for each pulse within the burst. The waveform is composed of 64 pulses with an LFM modulation, a pulse duration of 50 μs at 1.2 GHz centre frequency. Each PI is chosen randomly between [0.25, 0.75] ms and the initial phase of each pulse is chosen randomly. For processing of the irregular waveform, the irregular MTI clutter filtering is applied and the detection is performed by OMP combined with 2D matched filtering. Note that both waveforms have equal energy on target, i.e., equal number of pulses and pulse length, and they have both a dwell time of 32 ms.

The detection threshold is chosen for a probability of false alarms of 10-8. To account for migration artifacts, a detection is considered to be correct when the range and radial velocity are estimated within ±150 m and ±75 m/s, respectively, of the true target range and radial velocity.

3.2. SIMULATION RESULTS

The simulation results are presented and discussed in this subsection. The percentage of detected targets for the staggered medium-PRF waveform with linear processing is 11.8% compared to 73.5% for the irregular PI waveform with 2D matched filtering for 3000 Monte Carlo runs. The detection performance of the staggered medium-PRF waveform with linear processing is significantly less than the irregular PI waveforms with advanced processing. The performance degradation is partially caused by the three-pulse MTI clutter filter. Yet, a significant part of the performance degradation is due to the practical limitations of the staggered medium-PRF waveform with linear processing [5]. This part of the performance degradation may be solved by increasing transmit power, i.e., deploying a larger-sized system, however, the irregular waveforms with advanced processing may also offer a solution.

Figure 4 and Figure 5 show the detection histograms in range and velocity, respectively, for the staggered medium-PRF waveform and irregular PI waveform. The significant increase in detected targets can be noted even at large ranges. The detection histogram for the velocity is non-uniform for the staggered medium-PRF waveform, due to the practical limitations of linear processing. For the irregular waveforms with advanced processing, the detection histogram for velocity is uniform, as the 2D matched filter compensates for the velocity of the target.

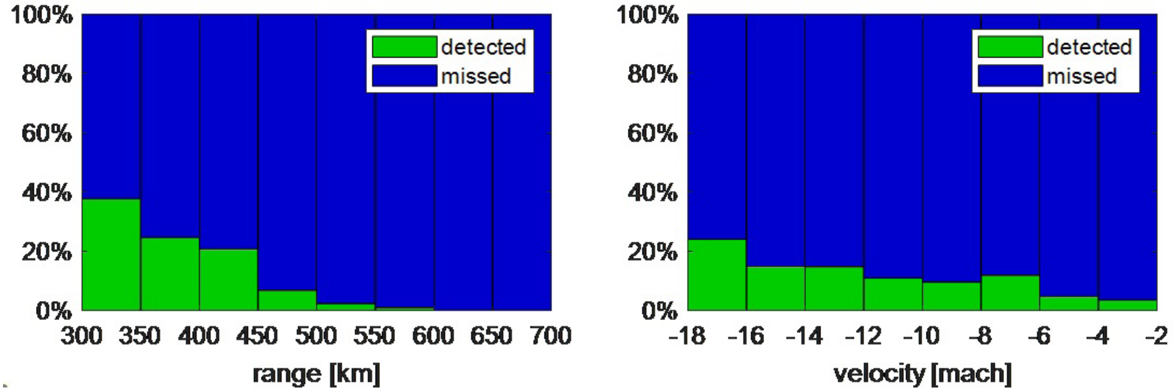


Figure 4. The detection histograms in range with (left) the staggered medium-PRF waveform with linear processing and (right) irregular PI waveform with advanced processing.

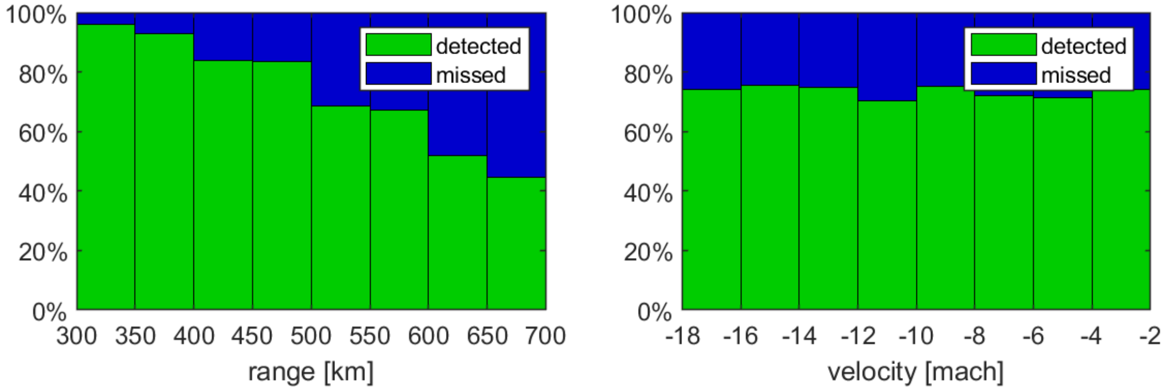


Figure 5. The detection histograms in velocity with (left) the staggered medium-PRF waveform with linear processing and (right) irregular PI waveform with advanced processing.

The bias of the range and velocity estimates of the target using the staggered medium-PRF waveform with linear processing are 8.56 m and -0.14 m/s, respectively, compared to -1.42 m and 0.02 m/s for the irregular waveform with advanced processing. The standard deviation of the estimates are 14.21 m and 7.08 m/s for the staggered medium-PRF waveform and 2.32 m and 1.10 m/s for irregular waveform. Clearly, our proposed irregular waveform and advanced processing improves the accuracy of the estimates roughly by a factor 6. Improved accuracy of the estimates improves radar tracker initialization and it increases the track accuracy.

The irregular waveforms and advanced processing significantly improves the detection range that can also be traded-off for shorter transmission times and/or usage of less transmit power. The shorter transmission time means that the freed radar time budget can be used for other tasks, e.g., more simultaneous active tracks. Decreasing the transmission power would allow for smaller-sized systems or improved energy/covertness profile of the sensor.

4. IRREGULAR WAVEFORMS AND ADVANCED PROCESSING IN THE CIVIL DOMAIN

The strength of irregular waveforms, or non-uniform sampling, combined with advanced processing has not gone unnoticed in the civil domain. In particular, advanced processing for imaging in medical and acoustic sensors and in radioastronomy have been matured and deployed in products. Within the medical imaging field, the usage of advanced processing significantly reduces the acquisition time, i.e., patient in the machine, while simultaneously sharpening the image. For example, Philips, General Electric and Siemens exploit it for MRI, CT, PET, and X-rays scanners [17], [18], [19]. Another field that highly benefits of sharpened images using advanced processing is in the acoustic domain. In particular, the oil and gas industry uses, e.g., seismic imaging, to geologically map the Earth's crust for natural resources [20]. Within radioastronomy, example of advanced processing for sharpened imaging and calibration can be found in the LOFAR and SKA telescopes [21], [22].

5. CONCLUSIONS

This paper has demonstrated the potential of waveforms consisting of irregular pulse intervals combined with advanced processing for the detection of hypersonic threats. In particular, we have shown that the novel waveforms and associated iterative 2D processing offer a potential solution to overcome the practical limitations of staggered PRF waveforms and linear 1D processing. Particularly for the hypersonic threat detection, this novel combination can significantly increase the detection performance in terms of the detection range and the accuracy of the estimated range and velocity measurements of the target. It has also been shown that the irregular MTI clutter filtering technique can sufficiently suppress the simulated sea clutter to be able to detect the hypersonic threats at large distances. Hence, the presented approach has the potential to significantly improve the detection range of the radar system and, simultaneously, it improves the track quality that can be constructed from these measurements. These advantages can contribute to early warning detection and increased time to engage hypersonic threats using radar systems.

Current efforts are focussed on thoroughly analysing the impact the usage of irregular waveforms and advanced signal processing within the complete radar processing chain and to improve robustness of these methods. In addition, the focus is on efficient implementations tailored to (specific) processing platforms in terms of computational load and memory capabilities. Moreover, designing waveforms in dynamic environments particularly for the hypersonic threats is an ongoing research topic.

ACKNOWLEDGEMENTS

The results in this paper are financed by the Ministry of Defence in The Netherland covered partially by the Nationaal Technologie Project MANDRAKE and the V1908 Radar Programma.

REFERENCES

[1] H. Astier, "Ukraine war: Russia fires hypersonic missiles in new barrage," on BBC News, Mar. 2023 [Online]. https://www.bbc.com/news/world-europe-64903202. [Accessed: 13 March 2023].

[2] NATO AVT-ST-008, "Assessment of the Status and Challenges Posed by Hypersonic Operational Threats", TR-AVT-ST-008, 2020.

[3] NATO AVT-359, "Impact of Hypersonic Operational Threats on Military Operations and Technical High Level Requirements Phase 1", STO-TR-AVT-359-Part-I, 2022.

[4] European Defence Agency, "Hypersonic Threat Detection and Countermeasures (Hypotenuse)", tender reference nr. 21.RTI.OP.092, Jul. 2021. https://etendering.ted.europa.eu/cft/cft-display.html?cftId=8915. [Accessed 13 March 2023].

[5] C. Alabaster, E. Hughes, and J. Matthew, "Medium PRF radar PRF selection using evolutionary algorithms," in IEEE Trans. on Aerospace and Electronic Systems, vol. 39, no. 3, 990–1001, 2003.

[6] A. De Maio, Y. Eldar and A. Haimovich, Compressed Sensing in Radar Signal Processing, Cambridge University Press, 2019.

[7] W. van Rossum and L. Anitori, "Simultaneous Resolution of Range-Doppler Ambiguities using Agile Pulse Intervals with Sparse Signal Processing," in IEEE Radar Conf., Florence, Italy, Sept. 2020.

[8] Defence advanced research projects agency (DARPA), "Beyond Linear Processing", notice id: HR001123S0008, Oct. 2022. https://sam.gov/opp/818c44d90f884834bf01e2e1382956ac/view. [Accessed 13 March 2023].

[9] L. Anitori and E. Joachim, "Waveform Design for Sparse Signal Processing in Radar." in Proc. of the IEEE Radar Conf., New York, NY, USA, 2021.

[10] M. Coutino and F. Uysal, "Reinforcement Learning for Radar Waveform Optimization" in Proc. of the 2023 IEEE Radar Conf., San Antonio, TX, USA, May 2023.

[11] L. de Martín and W. van Rossum, "Optimization of Pulse Intervals for Unambiguous Doppler Recovery with Oversampled Dictionary," in Proc. of the 2022 IEEE Radar Conf., New York, NY, USA, Mar. 2022.

[12] K. Klein, M. Coutino, R. Struiksma, P. Cox, L. Anitori, "Efficient Processing of Irregular PRF Waveforms: Clutter Suppression and Approximate 2D Matched Filtering" in Proc. of the 2023 IEEE Radar Conf., San Antonio, TX, USA, May 2023.

[13] P. Cox, M. Coutino, and W. van Rossum, "Kernel Design Meets Clutter Cancellation for Irregular Waveforms," in Proc. of the 2023 IEEE Radar Conf., San Antonio, TX, USA, May 2023.

[14] R. Struiksma, F. Uysal and W. van Rossum, "2D matched filtering with time-stretching; Application to Orthogonal Matching Pursuit (OMP)," in Proc. of the 18th European Radar Conf., London, United Kingdom, April 2022.

[15] M. A. Hadi, S. Alshebeili, K. Jamil, and F. E. A. El-Samie, "Compressive sensing applied to radar systems: an overview," in Signal, Image and Video Processing, vol. 9, no. 1, pp. 25–39, 2015.

[16] V. Gregers-Hansen and R. Mital, "An improved empirical model for radar sea clutter reflectivity," IEEE Trans. on Aerospace and Electronic Systems, vol. 48, no. 4, pp. 3512-3524, 2012.

[17] Philips Healthcare, "Snellere scans in alle lichaamszones met Compressed SENSE" [Online]. https://www.philips.nl/healthcare/artikelen/medisch-perspectief/compressed-sense. [Accessed 13 March 2023].

[18] General Electric Care, "HyperSense", [Online]. https://www.gehealthcare.com/-/jssmedia/files/us/non-gated/mri/hypersense-booklet.pdf?rev=-1&hash=FAE260A3F4CA0A82E236DEDA5CAD39A6. [Accessed 13 March 2023].

[19] Siemens, "Compressed Sensing: Beyond Speed", [Online]. https://www.siemens-healthineers.com/nl/magnetic-resonance-imaging/clinical-specialities/compressed-sensing. [Accessed 13 March 2023].

[20] Georgia Tech, "SINBAD," Seismic Laboratory for Imaging and Modeling, [Online]. https://slim.gatech.edu/projects/sinbadseismic-imaging-next-generation-basis-unctions-decomposition. [Accessed 13 March 2023].

[21] H. Garsden et al., "LOFAR sparse image reconstruction," Astronomy & Astrophysics, vol. 575, pp. 18, 2015.

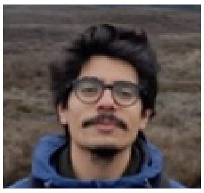
[22] ASTRON, "Calibration and imaging," [Online]. https://www.astron.nl/research-and-innovation/calibration-and-imaging/. [Accessed 13 March 2023].

Authors

Pepijn B. Cox has received his B.Sc. degree in Mechanical Engineering (cum laude) in 2010 and his M.Sc. degree in Systems and Control Engineering (cum laude) in 2013, both at the Delft University of Technology (TUDelft), The Netherlands. In 2018, he obtained his Ph.D. degree in the Control Systems group at the Eindhoven University of Technology (TUe), The Netherlands. In 2018, he was a postdoctoral researcher in the Control Systems group at the TUe.

Since 2019, he works as a signal processing expert at the Radar Technology group at TNO the Netherlands. Pepijn Cox's main research interests are in multistatic and netted radar systems, compressive sensing, numerical optimization, run-time verification as well as in linear parameter-varying and nonlinear system modelling and identification.

Keith T.J Klein received the M.Sc. degree in electrical engineering from Delft University of Technology, Delft, The Netherlands, in 2020. Since 2021, he has been with the Department of Radar Technology, Netherlands Organisation for Applied Scientific Research, The Hague, Netherlands. His current research interests include radar signal processing and radar system concepts.



Mario Coutiño received the M.Sc. and the Ph.D. degree (summa cum laude) in electrical engineering from the Delft University of Technology, Delft, The Netherlands, in July 2016 and April 2021, respectively. Since 2020, he has been a Signal Processing and Machine Learning Researcher with the Radar Technology Department, TNO, The Netherlands. He has held temporally positions with Thales Nederland, during 2015, and Bang & Olufsen, during 2016 working on inverse problems. His research interests include array signal processing, signal processing on networks, optimization, inverse problems, machine learning and radar technology. He was the recipient of the Best Student Paper Award at CAMSAP 2017, the CONACYT excellence scholarship and was a Visiting Researcher with RIKEN AIP and the Digital Technological Center at the University of Minnesota, in 2018 and 2019, respectively, working on graph methods and theoretical foundations of graph neural networks.

Dr. Laura Anitori received her Master of Science degree (cum laude) in Telecommunication Engineering from the University of Pisa, Italy, in 2005 and her Ph.D. degree (cum laude) in Electrical Engineering from the Technical University of Delft, The Netherlands, in 2013. Since 2007 she works at the Radar Technology department of TNO, The Netherlands, where she is senior scientist and program manager of the Defense funded radar research program. She is an IEEE senior member, member of the Board of Governors of IEEE AESS, and chair of the IEEE AESS Radar System Panel. She is government expert representative for The Netherlands within the European Defence Agency Radar Captech, and Dutch national representative in the NATO Sensors and Electronics Technology (SET) Panel. Her significant contributions to NATO were recognized with the SET Early Career Award in 2018, the 2019 SET Panel Excellence Award, and the NATO Scientific Excellence Award in 2022. She serves on several technical program committees and student competition committees at international scientific conferences.

DEFENCE ORIENTED TEST & EVALUATION CAPABILITIES AS ACCELERATOR FOR INNOVATION IN A TRIPLE HELIX ENVIRONMENT FOR MARINE ROBOTICS AND UNDERWATER APPLICATION

LT Francesco Cannarsa[1], LT Davide Cosimo[2], LT Lorenzo Bazzarello[3], LT Daniele S. Terracciano[4], Capt Navy (retd) Mirko Stifani[5]

Abstract

In recent years, Robotics and Artificial Intelligence have made significant improvements. The integration of these resources into the most sensitive areas can no longer be overlooked. It is increasingly important that the Test and Evaluation of these technologies be conducted collaboratively among Defence, Universities, and Industry, in a "Triple Helix" approach. This work presents ongoing and developing projects that aim to enhance the capabilities of maritime systems through the use of autonomous vehicles.

Keywords

EDA Innovation, HEDI, Underwater and Marine Robotics, MUS, Test & Evaluation.

1. INTRODUCTION

The Naval Support and Experimentation Centre (CSSN) of La Spezia is a Test and Evaluation Centre of the Italian Navy. It was created in 2007 combining the competencies of three technical centres of the Italian Navy: MARIPERMAN (standing committee for warfare materials), MARIMISSILI (centre for missile evaluation) and MARITELERADAR Livorno (centre for telecommunications evaluation). Test & Evaluation Capabilities (TECs) of CSSN are oriented to boost Logistic Support Engineer processes and experimentation and development of scientific-technological programs of the Italian Navy.

CSSN is hierarchically dependent on the Italian Navy Logistic Command, and its headquarter is based in La Spezia. Additional bases are also located in Portovenere focused on naval guns ranging, Livorno for electromagnetics/optics TECs (applied electronics, radar/infra-red signature, and electromagnetic compatibility), Nettuno as extension of Portovenere capabilities shared with Army, and Augusta the Degaussing/Deperming Station (SDDA) essential to protect Naval Units and Submarines against magnetic influence mines threat, supporting magnetic silencing. Thanks to its professionalism and scientific equipment, the Centre is a pole of excellence in the military and civilian fields, with skills and expertise unique in the national scene. To fulfil its institutional task, CSSN is structured into Departments, Offices, and Sections, supported by civilian and military employees and laboratories able to perform a wide range of tests including experimental tests, trials, qualifications, homologations and suitability for use of prototypes, materials, components and processes related to different science branches.

In particular the Experimental Department in La Spezia is in charge of the TECs in support of technical and

[1] UWW Office, CSSN, La Spezia, Italy francesco.cannarsa@marina.difesa.it

[2] UWW Office, CSSN, La Spezia, Italy davide.cosimo@marina.difesa.it

[3] UWW Office, CSSN, La Spezia, Italy lorenzo.bazzarello@marina.difesa.it

[4] UWW Office, CSSN, La Spezia, Italy danieles.terracciano@marina.difesa.it

[5] UWW Office, CSSN, La Spezia, Italy mirko.stifani@marina.difesa.it

experimental activities of the Naval Combat System (Missile and Artillery Sub-systems, Sonar and Torpedo systems, acoustic noise radiation from ships and submariners, unmanned system experimentations). It also manages experimental activities for Platform Systems (Propulsion System, hull, Generation, Distribution, and Conversion of Electric Energy and Safety).. The Department is divided into four Offices:

- Missile Weapon Office
- Artillery and Ammunition Office
- Underwater Warfare Office
- Platform Office

The Underwater Warfare Office (UWW) is responsible for technical and experimental activities related to underwater warfare systems and equipment, including testing and evaluation, certification, maintenance, and disposal at national and international levels. The office collaborates with nine Italian universities as part of the Interuniversity Research Centre ISME, with a focus on developing autonomous systems for the marine environment. The office also has positions for PhD officers on marine robotics, who attend the Information Department at the University of Pisa. Additionally, the office supports evaluations and studies of operational capabilities and new technologies in the sector of underwater innovation.

A similar collaboration applies with NATO STO CMRE (Centre for Maritime Research and Experimentation) hosted within the C.S.S.N. area to achieve the best possible synergy lining up the relative programs of work.

These capabilities have led CSSN to be one of the Test and Evaluation Centres of the European Defense Test & Evaluation Base of EDA, part of the Innovation Technology Network of the General Office on Innovation and Space of the Italian Navy General Staff and Test Centre of the NATO DIANA (Defense Innovation Accelerator for the North Atlantic). In this context, the Underwater Warfare Office became the natural embryo of the *Underwater Warfare National Hub*, a pole of aggregation for universities, private companies, and operative end-users, to accelerate the development of technologies.

In this context, a strong link is created between industry, academia, and the Navy, generating a Triple Helix Environment. Through this synergy, it is possible to establish a driving force capable of delivering high-level results through joint efforts and shared objectives. Within such an environment, it is easier to concentrate resources, materials, knowledge and hardware and software tools and laboratories, and share them to achieve increasingly difficult goals. Embracing this philosophy, two of the main projects of the UWW Office were born: BOOMER and CHOBIN. The first involves strong collaboration between Defense, the Academic World, and the Private Industry to develop concepts and create a mid-TRL (Technology Readiness Level) system of systems in the field of autonomous systems. The second project, on the other hand, benefits from the expertise of an excellence research centre: the NATO STO CMRE. Through the important know-how of this centre, efforts will be made to develop an interoperable and federated simulator focused above all on the underwater operations analysis issues including also autonomous systems.

1.1. BOOMER PROJECT

The BOOMER project is focused on creating a series of fifteen unmanned autonomous systems composed of different modules, which are connected to each other and can be reconfigured depending on the specific mission at hand. Each module typically contains one or more sensors that are used to gather and process data during the mission. One of the main objectives of the project is to create an open architecture that allows for collaboration between academia and companies. This architecture follows the "*frontseat-backseat*" paradigm [1], where one CPU controls the vehicle's actuators and receives basic commands, while another CPU in the payload is used for autonomous decision making. The project involved three private companies and the Interuniversity Research Centre ISME . Although the project has been concluded, future tasks envision the optimisation of underwater communication, improving the capability to exchange information and build complex tactical scenarios in a dedicated command and control station.

1.2. CHOBIN SIMULATOR

To enhance our testing capabilities and support design and development systems de-risking, it was also necessary a tool that could account for different environmental factors such as weather conditions, current intensity, and sensor range while updating outputs in real-time. A simulator with these capabilities would simplify the development of autonomous activity planning and rescheduling online. By incorporating the principles of Operations Analysis, existing simulators can be adapted to create an excellent Concept of Operation validator and autonomous optimization tools for underwater warfare scenarios. This system will enable CSSN to join NATO simulators and support their activities related to system and platform testing, evaluation, verification, and validation, as well as operations analysis. First phase of the project identified the Modeling & Simulation (M&S) requirements, which served as framework for the development of the simulator to be conducted during the second phase. By the Project's close (2024), a Simulator will be installed in CSSN laboratories. It will be possible to use it offline, online or link it to CMRE's Servers to work on a common closed network. The simulator will optimise time and reduce costs of development reducing the risk in a relevant environment. The simulator structure is based on the IEEE 1516-2010 (HLA) standard and is designed as a "federation" comprising multiple diverse components. Each component serves as an individual simulator or "federate". The federates share a run-time infrastructure (RTI) that offers various services, including information exchange, synchronisation, and federation management.

2. UXV'S EMPLOYMENT IN CRITICAL PICTURES

The doctrines falling under the scope of "Underwater Warfare" can be reviewed and addressed through the use of any type of unmanned systems/vehicle: aerial, surface or underwater (generically "UxS/Vs"). Thanks to the usage of Artificial Intelligence and miniaturisation of computer processors and sensors. UxVs have an increased level of autonomy [2] so the ability to make decisions by themselves. The knowledge acquired by the UWW Office of CSSN has therefore been employed to define the areas of application where underwater vehicles can be used and for what purposes. We wanted to describe below four "Critical" areas in which AUVs can be employed. Several experiments have already been conducted in this regard, and others are being prepared. Demonstrating the feasibility of using AUVs in such contexts could lead to rewriting the doctrine and significantly changing the procedures for using vehicles in naval and underwater contexts.

2.1. SEABED WARFARE

The recent damage of Baltic Sea gas pipes (part of the North Stream) at the end of September 2022 highlighted the vulnerability and exposure of numerous critical infrastructure to vital societal functions on a global scale such as safety, security, and economic stability. Power cables, telecommunications cables, and natural resource extraction networks are common targets of seabed warfare.

UxVs have also emerged as critical assets for infrastructure security in recent years. The development of novel sensors and automatic target recognition is critical for classifying potential undersea hazards. Artificial intelligence algorithms may provide a solution to this problem. Additionally, regular inspection and maintenance are essential in the oil and gas industry to ensure the safety of offshore equipment. Intruders, explosive and hazardous devices, naval mines, and unexploded ordnance are among the items that can be identified and tracked by their underwater surveillance capabilities.

In the near future, a network of underwater nodes formed of UxVs, in squad or swarming configuration, will be achieved to integrate ISR, ASW, NMW defence layers, structure under a distributed operation capability concept.

2.2. ASW

Historically, ASW operations have been carried out by manned platforms furnished with sophisticated and pricey sensors, which may be expensive and time-consuming above all in a challenging environment like the underwater. Maritime Unmanned Systems (MUS) can take the lead by collaborating with surface and underwater assets. A team of unmanned surface vehicles (USV) that monitors and controls Unmanned Underwater Vehicles (UUVs) conducting patrolling surveys might significantly improve the effectiveness of a port security system or critical infrastructure protection .

The increased interest in artificial intelligence has lately opened up new avenues for robot use. Unmanned systems are capable of carrying out higher-level activities and making decisions without the need for human assistance. By restricting the quantity of data that the vehicle must transmit, it is possible to bridge the communication gap that exists in the underwater channel. Furthermore, they enable continual management with the same degree of attention without succumbing to normal human stress situations.

During the exercise REPMUS-21 (Robotic Experimentation and Prototyping with Maritime Unmanned Systems), the Centre tested the use of UxVs for ASW purposes. Two underwater vehicles and one surface vehicle were used as nodes to implement a passive acoustic barrier, as reported in [3]. During REPMUS-22, a similar architecture with one more underwater asset and increased communication and detection capability was deployed.

2.3. MCM

Exploring seafloor to detect mines is a dangerous and time-consuming operation. The usage of UxV seems to be the key factor to improve this area. At CSSN, in cooperation with different ISME partners and NATO STO CMRE, we are improving the autonomy of single assets, enhancing underwater communications and underwater navigation capabilities. Regarding autonomy, the idea is to implement a directly on-board algorithm coming from Artificial Intelligence (A.I.), that thanks to ROS-based [4] open architecture, it can work on data collected in real time by the vehicle. In [5] and [6] is shown the online usage of Fast R-CNN to detect and localise small mine like bottom objects. In [7] another preliminary study of using saliency filters to detect anomalies in Sonar images is presented. The main purpose of this study is to match the ability of CNN to detect known objects, with the common usage in MCM field to consider and map also unknown objects, in this case using Saliency filtering.

Different navigation and communication tests were performed at the CSSN, results are presented in different reports: [8], [9] and [10]. The common path for developing this system is to have one or more surface unmanned vehicles, able to work as a gateway between underwater acoustic domain and surface radio frequency domain.

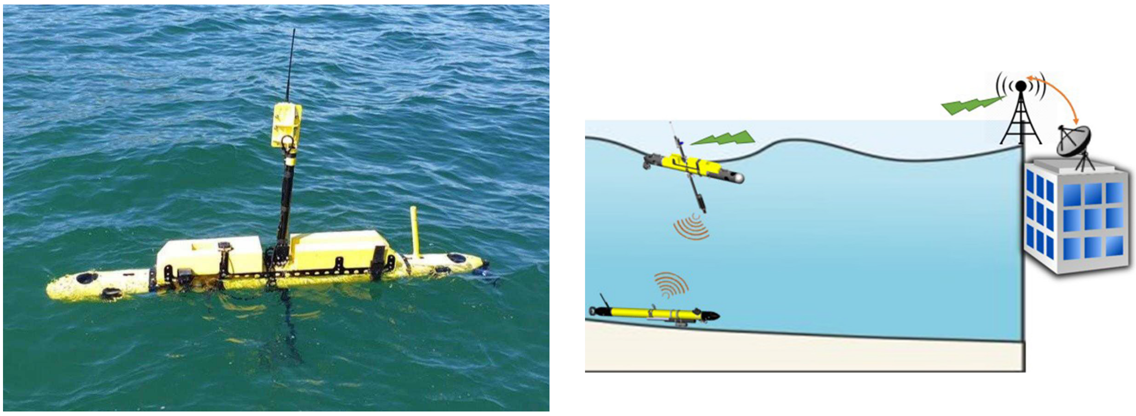


Figure 1. On the left, a mobile gateway buoy acting as a gateway between the underwater and radio frequency domains. On the right, a schematic of the communication flow.

During REPMUS-22 we perform on-fly mine-like object detection and localization, and thanks to the communication infrastructure and the usage of an Extended Kalman Filter we were able to sand this information directly for underwater vehicle to the onshore Control room.

2.4. REA

The REA (Rapid Environmental Assessment) scenario is designed to gather environmental data necessary for conducting operational activities and predicting key elements essential to its mission, such as the acoustic range of its sensors. The use of AUVs is highly suitable for this type of scenario. Deploying various vehicles in a wide area would allow for the monitoring of weather and environmental conditions in real time and without human effort. Studies of this kind are widely used in the environmental monitoring field and in studies such as oceanography, weather forecasting and sea state. The CSSN has conducted various tests with gliders and an USV. The gliders are equipped with CTD probes capable of recording the salinity and temperature of the sea at various depths. The surface vehicle is equipped with a weather station, DVL and a device for estimating the state of the sea. The USV is equipped to collect data and share it, via 4g, with an external server. During REPMUS-22, gliders and USV were used, cooperating with other nations and sharing the data collected with other exercise participants. Shared data permitted an operational coordination to recreate the situation at sea accurately during a simulated landing. Additionally, the data collected was shared with a NATO STO-CMRE server acting as a database, and made available to the CMRE's federated simulator. This allowed researchers to reconstruct the situation at sea faithfully on the simulator, opening up possibilities for simulation to run parallel and in real-time with the situation present in the field. Such applications align with the philosophy of the Digital Twin.

3. TEST & EVALUATION THROUGH OPERATIONAL ANALYSIS

The use of MUS has presented substantial and new challenges. In particular, Test and Evaluation (T&E) for unmanned systems is significantly more complex than for conventional systems due to their complexity and evolving maturity. These new technologies require specific T&E tools to assess them throughout their entire life cycle. Thanks to the University, numerous projects have been conducted in CSSN to address this need. T&E is the process of comparing a system and its subsystems against specific requirements, which is done through testing. Over the years, the UWW office of CSSN has acquired deep expertise in MUS and its sensors. This allows laboratory members to approach the problem with a robust, well-structured, and cost-effective process. MUS systems are not only the object of T&E but also fundamental to test and evaluate other systems, whether they are unmanned or not. All preparatory and research activities mentioned in Section [11] are necessary to carry out evaluations in a controlled environment. These activities have been the starting point for providing the laboratory T&E capabilities on different interconnected topics. The results obtained will be processed through 'Operations Analysis' [12] to understand, from an operational point-of-view, how MUSs contribute to obtain better results in a specific scenario minimising or maximising selected cost-functions.

3.1. VEHICLES INTEROPERABILITY AND INTEGRATION

UxVs have proliferated over the last few decades, but there are currently very few standards available. Indeed, the ability to share information, communicate and collaborate between heterogeneous assets could be a force multiplier, especially for the underwater domain.

In the SEALab context, we have found some key points useful to pursue the interoperability goal, for example using ROS open architecture middleware, trying to use a common command and control console, and actively contributing to major NATO standardisation projects such as Janus [13] for underwater communications and Common Autonomy Tasking Layer CATL [14] to have a common tasking language between heterogeneous vehicles.

An excellent opportunity to test these capabilities was provided by REPMUS-22, in which different research groups from many NATO countries independently implemented the ability to receive and transmit different tasks by CATL. The integration process starts with the definition of different user cases among the participants. The aim was to define a list of tasks, regardless of the medium used, and to identify which information is necessary and which is preferable to enable a vehicle to autonomously translate a given task into actions and, conversely, to translate what it perceives with its sensors into tasks. The final objective was to connect each vehicle to a communication broker so that it could receive or send tasks associated with other assets. During the whole exercise we were able to reach these results:

- connection to the communication broker provided by CMRE
- sending and receiving information concerning the various cooperating assets to our C2S;
- automatic routing of a detection to a cooperating vehicle provided by the CMRE team.

For the third target, despite the fact that no useful targets were found, a detection was simulated on 22 September. The message generated by the AUV containing information on latitude, longitude, depth and probability of being a mine was received acoustically by the USV, which sent it via a 4G connection to the C2S, which finally translated the information received into a CATL task. This task was routed by the system to a cooperative AUV of the STO-CMRE, called BIONDO, which was able to inspect an underwater object via an acoustic camera. In figure 2 the interoperability test performed during REPMUS-22 is depicted schematically.

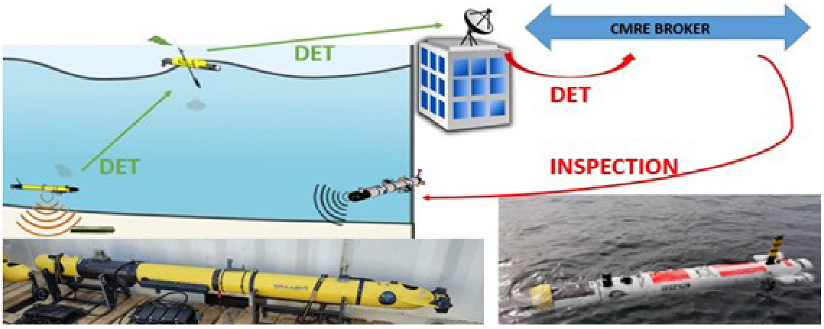


Figure 2. At sea architecture. Detection information created by an Automatic Target Recognition algorithm, is forwarded through a different link to CMRE CATL broker. This information is used to generate an inspection task for BIONDO vehicle.

3.2. DIANA

DIANA is a program launched by NATO that aims to accelerate the development of military technologies and solutions. DIANA focuses on several areas, including big data, artificial intelligence, quantum computing, biotechnologies, human enhancement, energy and propulsion, innovative materials, advanced manufacturing, hypersonics, and space [15]. The program seeks to identify and support promising technologies and solutions, providing funding, consultancy, and technical support to selected companies and organizations. Currently, there are 91 test centers that are part of the program and the CSSN is one of them. The approach used by DIANA involves the participation of industry, research, and defense, which allows for good results quickly and with reduced costs, as the "Quick Win" approach would suggest.

4. FUTURE DEVELOPMENT AND NEW CHALLENGES

As it was described in the previous chapters, TECs in a triple helix model with defence industry as prime characteristic are critical to maintain a technological advantage for new effective and safe systems. This leads us to consider that the TECs concept needs to be agile to keep pace with innovation that also requires a continuous learning culture and investment in training and development:

- Artificial intelligence, machine learning, and data analytics are at the beginning of their potential. A proper and consolidated use of such technologies can continuously update the way TECs are conducted. From faster and more accurate data analysis it is possible to obtain more efficient testing and better decision-making in connection with the M&S concept.
- Family2System of Systems: the increasing complexity of defence systems TECs need to consider capabilities objectives to test and evaluate the interoperability and interchangeability of different systems. This requires M&S to maximise and/or minimise multiple parameters of the full life cycle model.
- International cooperation is essential to provide new opportunities for innovation and cost-sharing for TECs, dissemination of culture and better decision-making.

Nevertheless, new challenges arise related to data privacy, intellectual property rights, cybersecurity, coordination between different regulatory frameworks and ethical considerations. A collaborative approach is mandatory to manage technologies and challenges they present.

5. CONCLUSIONS

Collaborative efforts between Academia, Private Industry, and Defense have the potential to achieve excellent results within a reasonable timeframe, provided that commitment is focused on a shared goal. Until recently, CSSN's abilities in the field of autonomous vehicles were non-existent. However, through targeted projects with appropriate funding, significant advancements have been made in the use of unmanned and autonomous vehicles for Defense. Moreover, the potential for further growth in this field is still very high and future projects hold promise for even more significant results. In a global context where resources are limited, establishing partnerships between various entities is critical to promoting efficient research. Therefore, it is imperative that these partnerships be done to leverage the collective strengths of these different entities in pursuit of shared objectives.

REFERENCES

[1] Benjamin M., Leonard J. Schmidt H., Newman P., "A Tour of MOOS-IvP Autonomy Software Modules", 02 2009

[2] Dugelay S., Connors W., Furfaro T. and Baralli F., (2016) "Collaborative Autonomy for Mine Countermeasures", NATO STO-CMRE.

[3] Bazzarello L. et al. (2022,Jun) "Remote Passive Acoustic Barrier with Maritime Unmanned Systems: preliminary tests during REPMUS-21.", International Conference on Ship & Maritime Research

[4] https://www.ros.org/.

[5] Zacchini L. et al. (2022) "Autonomous Underwater Environment Perceiving and Modeling: An Experimental Campaign With FeelHippo AUV for Forward Looking Sonar-Based Automatic Target Recognition and Data Association", IEEE Journal of Oceanic Engineering, Vol. 1, pp. 1-20.

[6] Topini A. et al. (2022) "Autonomous underwater environment perceiving and modeling: an experimental campaign with FeelHippo AUV for Forward Looking Sonar-based Automatic Target Recognition and Data Association.", I-RIM Italian Conference on Robotics and Intelligent Machines.

[7] Bazzarello L., Pulpito O., Cannarsa F., Bresciani M., Costanzi R., Acito N., Diani M., Corsini G., Caiti A.. (2022) "Anomaly detection in Sonar images: application of saliency filters", Metrology for the Sea.

[8] Bresciani M.,Peralta G., Ruscio F., Tani S., Manzari V., Bazzarello L., Caiti A. and Costanzi R. (2021) "ASV acoustically tracking and following an AUV: preliminary experimental evaluation", OCEANS 2021: San Diego – Porto, Vol. 1, pp1-7.

[9] Bresciani M. et al. (2021) "Localisation Approaches for Underwater Autonomy within the EUMarineRobots H2020 project: experimental activity at SEALab", OCEANS 2021: San Diego – Porto.

[10] Bresciani M. et al., (2008) "Cooperative ASV/AUV system exploiting active acoustic localization", 2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pp 4337-4342.

[11] Terracciano D.S., Manzari V., Stifani M., Allotta B., Caiti A., Casalino G.(2019,Oct) "SEAlab current research trends: Maritime Unmanned Systems for dual-use applications", International Workshop on Metrology for the Sea

[12] Wagner, D.H. and Mylander W.C. and Sanders,T.J. (1999). "Naval Operations Analysis", Naval Inst Pr.

[13] Potter J., Alves J., Green D., Zappa G., McCoy K., Nissen I., (2014) "The JANUS underwater communications standard", Underwater Communications and Networking, UComms.

[14] Furfaro T., et al., (2021) "A Task-Centric Messaging Model for Federated Autonomous Collaboration", Fifth Underwater Communications and Networking Conference (UComms).

[15] https://www.diana.nato.int/

Authors

LT Francesco Cannarsa

LT Francesco Cannarsa is an Engineer Officer at the Naval Support and Experimentation Centre of the Italian Navy, in La Spezia. He received the M.Sc. degree in Telecommunications Engineering in 2017 from the University of Pisa. He is part of CSSN Underwater Warfare Office since September 2021. He is assigned at New Systems Section.

LT Davide Cosimo

LT Davide Cosimo is an Engineer Officer at the Naval Support and Experimentation Centre of the Italian Navy, in La Spezia. He joined the Italian Navy in 2010 and completed the Naval Academy of Livorno in 2014. He received the M. Sc. degree in Telecommunications Engineering in 2017 from the University of Pisa. He is part of CSSN Underwater Warfare Office since November 2022. His principal task is torpedo analysis.

LT Lorenzo Bazzarello

Lorenzo Bazzarello is an Engineer Officer at the Naval Support and Experimentation Centre of the Italian Navy, in La Spezia. He received the M. Sc. degree in Telecommunications Engineering in 2013 from the University of Pisa. From 2013 to 2019 he was part of the research branch in the Mine Counter Measure headquarter of the Italian Navy. In 2015 he attended the course in Mine Counter Measure at the Naval Academy of Livorno. In 2017 he received a postmaster degree in Underwater Electroacoustics and Application at the University of Pisa. He started his Ph.D. program in Underwater Electroacoustics and Robotics, in November 2019. His research interests include high frequency imaging sonar, acoustic measurement techniques, electroacoustics, artificial intelligence applied to mine counter measure, underwater robotics.

LT Daniele S. Terracciano

LT Daniele Terracciano is an engineer officer at the Naval Support and Experimentation Centre (CSSN) of the Italian Navy, in La Spezia. He joined the Italian Navy in 2006 and he completed the Naval Academy of Livorno in 2010. He received the M. Sc. Degree in Telecommunications Engineering in 2013 from University of Pisa. He served as the Combat System manager on Italian Navy ships and at the Augusta (Sicily) naval base, from 2013 to 2017. He has been employed by CSSN (La Spezia) since 2017. In September 2021, he obtained the PhD degree in Information Engineering from the University of Pisa. Actually, he works as the Head of Underwater Detection Section within the Underwater Warfare Office of the CSSN.

CAPT IT Navy (retd) Mirko Stifani

Mirko Stifani received the postgraduate advanced course in underwater electroacoustics and its applications from the University of Pisa, Italy, in 2005. He joined the Italian Navy in 1993 and completed the Naval Academy of Livorno in 2000. He was the Chief of the Underwater Warfare Office with the Naval Support and Experimentation Centre of the Italian Navy, La Spezia, Italy and the Director of the SEALab, La Spezia, Italy until march 2023. Currently he is Product Leader Unmanned Systems at Fincantieri NexTech.

ACKNOWLEDGEMENTS

EDA would like to express its sincerest gratitude to all the participants of the *EDA Research, Technology, and Innovation Best Papers Award 2023*. Their contributions and dedication have been instrumental in identifying the most innovative and exceptional ideas among the submissions making this contest a remarkable success.

Furthermore, their passion for research, technology, and innovation serves as a continuous source of inspiration, shaping the future of the EU Defence capabilities for tomorrow.

Evaluation Committee Members (sorted alphabetically):

- **Daniel MOSQUERA,** Project Officer Air Systems Technologies
- **Dr. Fabrizio BERIZZI,** Project Officer Optronics Technologies
- **Dr. Panagiotis KIKIRAS,** Head of Unit Technology and Innovation
- **Zsolt NAGY,** Policy Officer Strategic Analysis

Reviewers (sorted alphabetically):

- **Dr. Constantinos HADJISAVVAS,** Project Officer Energy
- **Dr. Eleni PATOUNI,** Project Officer Emerging GNC Technologies
- **Dr. Giorgos DIMITIOU,** Project Officer Offshore Energy
- **Dr. Giuseppe DAQUINO,** Project Officer Materials & Structures Technologies
- **Dr. Patrick LANGLOIS,** Project Officer Components Technologies
- **Dr. Rolf MICHELS,** Project Officer Innovative Advanced Materials

Supporting staff (sorted alphabetically):

- **Alejandro ARROYO,** Innovation Management Trainee
- **Andrea WILHELMOVA**, Procurement and Grant Officer

For more information about the European Defence Agency,
please see our website: www.eda.europa.eu
and our biannual magazine, European Defence Matters

ISBN: 978-92-95075-79-5
DOI: 10.2836/568224

EUROPEAN
DEFENCE
AGENCY

QU-04-23-542-EN-N

European Defence Agency
Rue des Drapiers 17-23
B-1050 Brussels - Belgium

www.eda.europa.eu

Tel +32 2 504 28 00
info@eda.europa.eu

Publications Office
of the European Union

ISBN 978-92-95075-79-5