14th International Defense and Homeland Security Simulation Workshop, 007
21st International Multidisciplinary Modeling & Simulation Multiconference

2724-0363 © 2024 The Authors.
doi: 10.46354/i3m.2024.dhss.007

An Audacious Wargame on Critical Infrastructures based on LLMs and Simulation over Physical, Cyber & Cognitive Actions

Agostino G. Bruzzone[1,2] *, Antonio Giovannetti[1,2], Luca Cirillo[1], Marco Gotelli[1,3], Filippo Ghisi[1,2]

1Simulation Team, Via Cadorna 2, Savona, 17100, Italy
2SIM4Future, via Trento 43, 16145 Genova, Italy
3DIME, Genoa University, Via Opera Pia 15, Genova, 16145, Italy

*Corresponding author. Email address:agostino.bruzzone@simulationteam.com

Abstract

This paper proposes an AuW (Audacious Wargaming) Solutions that allow to be immersed in Critical Infrastructure Protection over the different dimensions: physical, virtual and cognitive. In particular the proposed approach is combining use of eXtended Reality through our Multi Domain Chessboard dynamically connected with a Stochastic Discrete Event Simulator driven by Intelligent Agents and integrated with our Brain Module devoted to generate and analyze cognitive actions over BPSM (Broadcasting, Print & Social Media). The wargame is called CW-Brainware and it is devoted to protect Energy and Communication Critical Infrastructures on land area from Threats respect its Vulnerabilities. The domains include air, land, space, cyberspace, but some threats could arrive even from sea, while the Cognitive Actions are generated on the Authorities, Personnel, Local and Domestic Population as well as on the Infrastructure themselves to introduce bias with local population.

Keywords: Audacious Wargames, AI, Modeling and Simulation, LLM

1. Introduction

The security and resilience of strategic critical infrastructures are increasingly threatened by diverse and evolving challenges, the integration of advanced methodologies such as audacious wargaming and cognitive warfare is becoming essential. Strategic critical infrastructure protection demands innovative approaches that can anticipate and counteract both conventional and unconventional threats. Indeed, audacious wargaming is thought in order for participants to explore nontraditional and innovative scenarios that are particularly significant in multi domain operations – land, sea, air, cyber, space - . The cognitive is nowadays included as one of the dimension to be taken into account when defining a scenario adding a psychological and information-based layer to the traditional concept of warfare, targeting the decision-making processes of adversaries.

Furthermore Recent developments in simulation-based military training and the application of data analytics and machine learning in large-scale projects have underscored the importance of these approaches.

As highlighted by Bruzzone et al. (2023), the sustainability, environmental impacts, and resilience of strategic infrastructures require continuous adaptation to new threats, leveraging advanced simulation and intelligent systems. Moreover, the necessity for NATO and allied nations to develop future strategic engineers, points to the critical need for expertise in these areas to safeguard national security interests.

This paper explores the intersection of audacious wargaming and cognitive warfare within the broader framework. It aims to demonstrate how these methodologies are ready be integrated into strategic planning and operational readiness to enhance the protection of vital infrastructures. By examining the latest research and practical applications, this study seeks to contribute to the ongoing discourse on the future of strategic infrastructure defense in an increasingly complex and contested global environment.

Strategic Critical Infrastructure Protection is affecting many elements therefore it is evident that is strongly related with Energy Source (e.g. Power Plants, Renewable Sources, Hydro Plants), Power Grid as well as with Communications. It is evident that the vulnerabilities to these aspects could have a drastic impact on the Society and Economy by blocking industrial activities.

2. Threats and Criticalities

The resilience of critical infrastructure faces an increasingly complex array of threats spanning multiple domains—land, sea, air, cyber, space, and cognitive—each contributing uniquely to the vulnerabilities of essential services like energy, transportation, healthcare, and communication(George et al., 2024). Infrastructure resilience, traditionally focused on physical robustness, must now adapt to the evolving nature of both kinetic and non-kinetic threats. On land, physical sabotage through terrorism or insurgent activity continues to be a primary concern, particularly regarding transportation networks, power grids, and industrial facilities. The use of autonomous underwater and surface vehicles by adversaries has heightened the complexity of protecting maritime infrastructure(Miętkiewicz, 2018).

Airborne threats, including both traditional military aircraft and unmanned aerial vehicles (UAVs), are becoming more prevalent in targeting infrastructure such as airports, energy plants, and communication towers. These aerial attacks could disable or severely disrupt operations with precision strikes (Chaturvedi et al., 2019). Moreover, cyber threats are becoming one of the most critical concerns for infrastructure resilience. The increasing reliance on interconnected, digital systems exposes infrastructure to cyber-attacks that could cripple essential services without the need for a physical presence (Zhang et al., 2020; Kontouras et al., 2017) .

Space-based assets, including satellites responsible for communications, GPS, and remote sensing, play an increasingly pivotal role in the functioning of global infrastructure. In the cognitive domain, disinformation and psychological operations (PsyOps) undermines public trust in the resilience of critical infrastructure.

It is necessary not only to design and engineer these infrastructures to be robust respect accidents as well as resilient versus malicious actions and threats, but also to prepare Managers and Decision Makers to understand this framework and learn how to deal with it. The threats are obviously physical such as High Yield Explosives destroying a Power Plant or a Graphite Bomb generating short-circuits by the creation of dense clouds of very fine carbon filaments that compromise the natural insulation by air of high voltage plant elements (e.g. Power lines, transformers).

These actions could be carried out by antagonists, terrorists, sabotages, members of fifth column as well as organized forces using mortars, cannons, drones, etc. In addition and combination it is possible to conduct cyber-attacks to these infrastructures compromising their operative capabilities and/or even damaging physical them by activating improper procedures through manipulation of software and data.

It is even important to consider the cognitive actions over Broadcasting, Press and Social Media that could produce damages to the personnel and management people dealing with operations and/or protection of the Critical Infrastructures, but even to promote hostile attitude of the population against them claiming about pollution, health threats, damages to the environment as well as to other activities (e.g. tourism). These actions could be aggressive by our opponents and antagonists, but also positive correcting effects of cognitive attacks or improving our resilience, by our resources as well by allied and/or population if it has developed critical capability to address these problems (Claverie et al., 2022) .

In a crisis or pre-crisis situation a decision maker could get overloaded by the workload required to address all these problems and usually the people in charge of protecting these infrastructures at high level have just personal experience and natural talent to address these issues in personal ways. The idea of the author has been to create a wargame able to allow Decision Makers to experience these context, turn familiar with the related dynamics and to play supported by AI over the different domains without getting lost in the complexity.

Modeling and simulation play a crucial role in preparing decision-makers for the increasingly sophisticated threats to critical infrastructure across multiple domains. With threats becoming more complex and interconnected—ranging from physical sabotage to cyberattacks and cognitive warfare—

traditional methods of crisis response are insufficient. Simulation tools offer a controlled environment to test various threat scenarios and explore the cascading effects of failures across interconnected systems. By modeling real-world infrastructures and simulating both kinetic and non-kinetic attacks, these tools provide invaluable insights into vulnerabilities and potential mitigation strategies (Wiseman et al., 2014).

Simulation Team's research on **CAPIAS** (Cables, Pipelines, Marine Infrastructures & Autonomous Systems) has been instrumental in advancing infrastructure protection strategies. Using advanced AI-driven models, such as **HBM** (Human Behavior Models) and **LLMs** (Large Language Models), these simulations capture not only the physical and digital threats but also the human decision-making processes under stress (Bruzzone et al, 2023; Bruzzone et al., 2017; Bruzzone et al., 2011). AI technologies enhance the accuracy and adaptability of simulations, offering decision-makers the ability to model diverse scenarios and outcomes in real-time. For example, modeling the effects of a cyberattack on power grids reveal how cascading failures in one sector might trigger disruptions in others, such as transportation and healthcare. However, the cognitive impact of misinformation campaigns targeting infrastructure operators or the public is simulated to assess how psychological and social variables influence crisis outcomes (Bruzzone et al., 2014a; Bruzzone et al., 2014b).

These simulations are not just about crisis management but also about building resilience. They allow leaders to explore proactive strategies, test response protocols, and understand the interdependencies between physical and digital infrastructures, which are often overlooked. By repeatedly engaging in simulated scenarios, decision-makers become better equipped to respond to real-world crises, having already experienced the decision paths, consequences, and risk mitigations through these advanced models (Mazal et al., 2019; Hodicky et al., 2021).

Wargaming has emerged as a powerful tool for educating decision-makers on the complexity and interdependence of threats to critical infrastructure. Unlike traditional crisis management exercises, wargames immerse participants in simulated multi-domain conflicts where they must navigate physical, cyber, and cognitive threats simultaneously . The introduction of AI-driven tools like **CW-SINON** (Cognitive Warfare Simulation, AI, and Neural Networks) has revolutionized wargaming by incorporating complex human behavior and cognitive factors, which are critical in modern warfare . These wargames are designed not just to simulate military conflicts but to explore how decision-makers handle the overwhelming complexity of protecting infrastructure in the face of coordinated attacks from adversaries (Cayirci et al., 2022; Hodicky et al. 2022; Hodicky. et al., 2017)).

The use of AI in wargaming enables decision-makers to play through different scenarios that include both conventional attacks, such as physical sabotage, and non-kinetic strategies like disinformation campaigns. For example, a wargame might simulate an adversary launching a cyberattack on a power plant while simultaneously spreading misinformation through social media, causing public panic. In such scenarios, decision-makers must balance immediate operational responses with managing public perception and preventing societal disruption. The **CAPIAS Wargame**, focused on offshore strategic assets, has demonstrated the value of this approach, enabling leaders to experience and manage the dynamics of multi-domain threats in a realistic, consequence-free environment.

3. CW-BRAINWARE: Audacious Wargaming

CW-BRAINWARE (Cognitive Wargame, Behavioral Response Analysis and Integrated Network simulation for Wargaming Experience) is an innovative Solution based on the combined use of AI & M&S to support the Decisions related to Multi Domain Threats to be carried out on very Complex Scenarios that involve Kinetics, Cyber & Cognitive as well as Hybrid Warfare while protecting critical Infrastructures . This is an AuW (Audacious Wargaming) & Simulator able to develop capabilities in using the BPSM (Broadcasting, Print & Social Media) in Defensive and Offensive Way by MS2G (Modeling, interoperable Simulation, Serious Games) & AI, automatically supporting the Full Understanding of Opponent Strategies and Optimizing Actions. CW-BRAINWARE is an AuW (Audacious Wargaming) Solution devoted to deal with a game over a complex, dynamic environment where multiple decision-makers engage in cyber, kinetic and cognitive warfare to influence both military forces and civilian populations. Each decision-maker maneuvers through a landscape of attacks that affect the social, psychological and emotional parameters of their adversary societies. Participants must also contend with incoming assaults from opponents, necessitating responsive strategies, including the issuance of both genuine and deceptive public statements to manipulate the emotional climate of their own forces and citizens. The simulator integrates demographic variables such as ethnicity, age, gender, religion, political orientation, health status, educational background, income levels, and social affiliations to realistically model human emotional responses to conflict scenarios as well as cognitive factors such as moral, motivation, integrity, beliefs, values et cetera. This facilitates strategic planning and decision-making, offering a holistic view of potential public sentiment in reaction to urban development projects and warfare tactics. Players choose their side, with its specific cognitive, social and demographic factors. Players plan their actions, choosing between cognitive, cyber, kinetic and cognitive attacks targeting either military forces or

civilian populations of their adversaries.

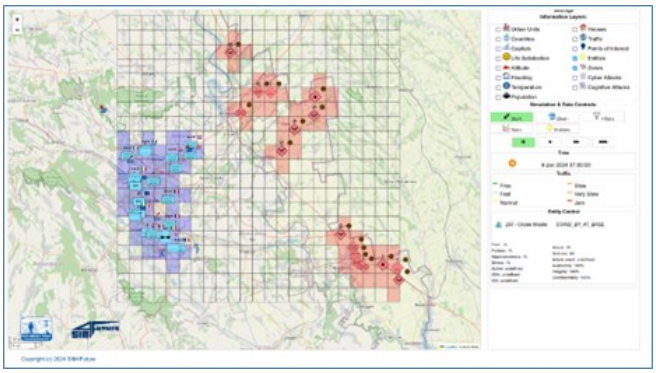

Fig.1 – CW-BRAINWARE Simulation

Fig.3 – CW-BRAINWARE interface

They must allocate resources for defense against incoming attacks and protect their Critical Infrastructures. The selected COA (Course of Action) are Implemented by Intelligent Agent developing strategies of Players. The Simulator evaluates the vulnerabilities of the Critical Infrastructures to the attacks and calculates impacts even considering the chosen tactics, affecting cognitive, psychological and emotional states of virtual troops and populations. Players prepare and deliver cognitive actions, based on true or deceptive news to manipulate the emotional response of population and troops. CW-BRAINWARE simulator provides feedbacks on the consequences of all actions. Including changes in public sentiment and military morale, allowing players to adjust their strategies by using AI and LLMs.

$$I_{society} = \frac{I_{wind,p} \cdot w_{wind} + I_{solar,p} \cdot w_{solar} + I_{thermal,p} \cdot w_{thermal} + I_{telecom,p} \cdot w_{telecom}}{w_{wind} + w_{solar} + w_{thermal} + w_{telecom}}$$

Where:

- I represents the level of integrity of the energy plant or infrastructure
- w represents the relative weight the energy plant or infrastructure

Fig.7 – CW-BRAINWARE Message Manager to generate cognitive attacks thanks to the use of instruct LLMs

CW-BRAINWARE is an innovative wargame addressing Cognitive, Cyber and Hybrid Warfare and it was created by Simulation Team by combining Modeling & Simulation, with a focus on Human Behavior Modeling, cutting-edge Artificial Intelligence, particularly Generative AI and Large Language Models (LLMs) as well as immersive Virtual Reality. By this approach CW-BRAINWARE offers an uniquely captivating and comprehensive Strategic Experience on using AI in Cognitive Warfare on Defensive and Aggressive Ways. Through the simulation of realistic demographic, psychological, cultural and socio-political environments, players develop strategic decision-making skills that are crucial in managing effectively multi-faceted and multi-layer modern Conflicts. This Wargame challenges participants to master the art of using AI in cognitive warfare, to compromise Critical Infrastructures, defend Population, understand the dynamics as well as forecasting of community reactions. This support the development of capabilities dealing with high-stakes, real-time decision-making required by the dynamics and complexity of real-world cognitive warfare.

4. Strategic Wargames leading to Wisdom

CW-BRAINWARE allows to consider Strategic Aspects for Decision Makers such as Politics, Intelligence, Level of Conflicts and Future Impacts and Risks related to compromission of Critical Infrastructures from both Physical and Virtual Point of View as well effects of Cognitive Actions. By integrating political, intelligence, and conflict level considerations, these simulations allow leaders to anticipate future impacts and assess the vulnerabilities of critical infrastructures from both physical and virtual perspectives. In a world where cyberattacks and cognitive warfare—such as disinformation campaigns or psychological operations—are increasingly shaping the landscape of global security, wargames offer a controlled environment to explore and mitigate such multifaceted threats. These simulations not only

enable a deeper understanding of the immediate tactical challenges but also illuminate the broader strategic consequences of decision-making. By testing various scenarios, decision-makers learn how to build resilience against the compromission of essential infrastructures, analyze the effectiveness of response strategies, and ultimately foster wisdom in balancing short-term security needs with long-term stability. Through this strategic foresight, wargames like those enabled by CW-BRAINWARE bridge the gap between theoretical knowledge and actionable insights, enhancing both preparedness and adaptability in an increasingly interconnected and contested world.

5. Wargaming in Multi Domains and Dimensions

CW-BRAINWARE is an Innovative Wargames that works on 5 domains (Land, Sea, Air, Cyberspace & Space) considering Kinetic, Cyber and Cognitive attacks on troops and Critical Infrastructures

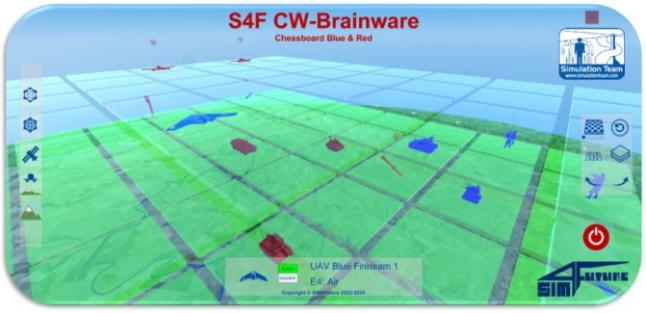

Fig.2 – CW-BRAINWARE Multidimension Chessboard

There is a Common Scenario with Operations simulating troops, while each Player (Blue & Red) has a CW-BRAINWARE Chess Board controlling 10 units over a 6 dimensional map and over different other chessboard (e.g. Political/Intelligence/Social Catalysts, Escalation Tables, Future Risks) and a BRAINS interface to generated, decode and counter cognitive actions by using the CW-BRAINWARE LLMs

CW-BRAINWARE is mostly operating over land, air, space and cyberspace domain, therefore also a small Naval component is present to be used to conduct cruise missile attacks against Critical Infrastructures and Forces on the Scenario that is located in an area corresponding to Moldova. The Player assign high level tasks to units that are directed to accomplish their Missions by Intelligent Agents, while the LLMs analyze the cognitive actions and antagonist initiatives and propose reactions

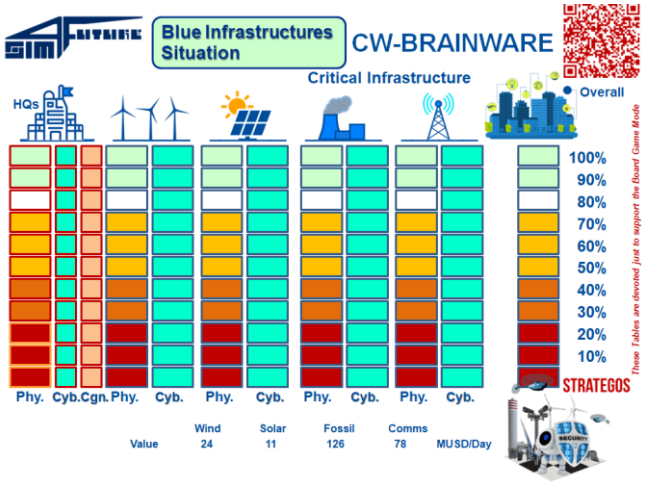

Fig.5 – CW-BRAINWARE Dashboard on Current Status

6. Scenario

CW-BRAINWARE operates on a near future Scenario where Critical Infrastructures for Energy and Communications should be protected by Blue in an area corresponding to Moldova against Red Contractors operating into an area unofficially under their control to destabilize the remain of the Country. Traditional Assets (Armored Infantry, APC ***Armored Personnel Carrier***, SPH ***Armored Personnel Carrier*** & SAM Surface Air Missiles), SOF Special Operations Forces while UAV, UGV, UCGV & UCAV (Unmanned Ground Vehicles, Unmanned Arial Vehicles, Unmanned Combat Ground Vehicle, Unmanned Combat Arial Vehicle) are extensively used.

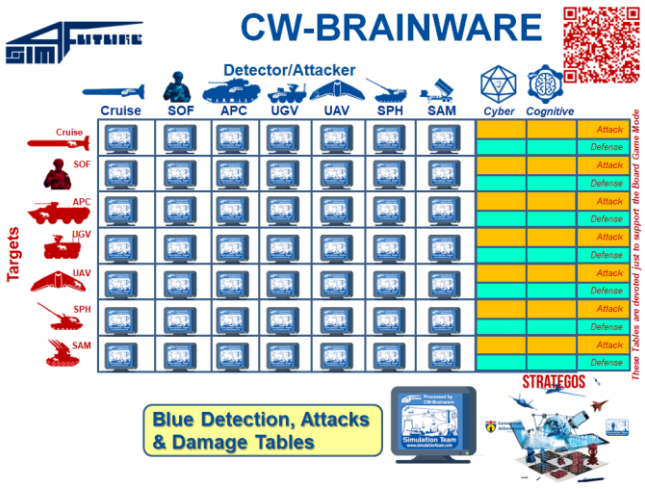

Fig.4 – CW-BRAINWARE Interactions among Unities

7. Multi Domain Chessboard

CW-BRAINWARE is easy to play and provide the flavor of the complexity of modern Cognitive, Cyber and Kinetic Warfare for a Commander that have Critical Tasks to protect Strategic Critical Infrastructures necessary to the Global Plan and to don't destabilize a Country, an Area or the Domestic Opinion respect the overall Goals

CW-BRAINWARE combines multiple Domains and Multiple Dimensions introducing Commanders in the complexity to protect Critical Infrastructures respect attacks of SOF (Special Operations Forces) and Drones as well as Cyber Actions and Cognitive Attacks.

CW-BRAINWARE Chessboard allows to control few high entities to define offensive and defensive strategies as well as to plan kinetic, cyber and cognitive attacks to Troops and Critical Infrastructures focusing on a single domain or on the whole combined multidomain

8. Cognitive Actions on People and Infrastructures

CW-BRAINWARE allows to move from Operational View to High Tasks Assignments as well as to counter actions on BPSM related to Cognitive Attacks. The effect of Cognitive attacks is visible on the Troops, on the Map as well as on Domestic Opinion. The LLMs give interpretations to understand the info targets and Goals of the Antagonists as well as suggestion for smart reactions in terms of cognitive vectors and messages. In the context of cognitive attacks, various Large Language Models (LLMs) (different solution available, also Open Source Models) are implemented, using techniques such as Retrieval-Augmented Generation (RAG) to interpret specific topics and provide tailored responses. These models, known for their zero-shot learning capabilities, allow for context-sensitive messaging without requiring prior training on the exact task. The process begins with the user crafting a prompt and selecting the preferred media platform (social media, newspapers, or television), alongside parameters such as tone, formality, emotionality, the inclusion of deep fake content, and the allocated budget. The budget allocation plays a pivotal role in determining the reach and impact of the message, particularly when choosing between major media outlets or broader social media dissemination.

Once the AI generates the message, the user is enabled either to modify it or send it as it is directly. In addition, the system provides emotional variables, allowing the user to gauge the emotional resonance of the content. Sentiment analysis is then performed to optimize the message's effectiveness, suggesting adjustments that could enhance its appeal to specific audiences. Depending on the message content, tone, and medium, the message could be directed toward different clusters of people. For example, emotionally charged or deep fake content may attract wider attention, yet in populations with higher education levels, such messages might trigger skepticism or even backlash. The System generates in addition counter cognitive attacks tailored responses to the user message. The propagation of the information is modeled using the Simulation Team Information Propagation Model, which provides insights into how the message spreads across various networks and audiences. This approach allows users to better understand the reach and influence of their cognitive operations, making it a powerful tool in strategic communication and psychological warfare. The model accounts for emotional variables, cluster segmentation, and media channels to create a more precise and adaptable cognitive attack strategy.

9. Conclusions

CW-BRAINWARE is a very innovative wargame that combines multiple models into a single framework very easy to play and able to immerse the user in the context and to develop his own winning strategies in this complex problem. The use of LLM for supporting the human players one against the other is a very promising opportunity to develop the knowledge based to generate other games as well as Lesson Learner Smart Actors and AI based Decision Support Systems. This multi-layered approach enables adaptability and foresight, allowing for real-time adjustments based on target audience responses and different threats. The fusion of AI, strategic simulations, and advanced propagation models creates a powerful tool for governments and organizations, enhancing their ability to engage in multi-domain and multi-dimension operations with a deeper understanding of the potential effects.

References

Bruzzone, A. G., Massei, M., Gotelli, M., Giovannetti, A., & Martella, A. (2023). Sustainability, Environmental Impacts and Resilience of Strategic Infrastructures.

Mazal, J., & Bruzzone, A. G. (2019). NATO needs of Future Strategic Engineers. In *Workshop on Applied Modelling & Simulation* (Vol. 35).

Bruzzone, A. G., & Massei, M. (2017). Simulation-based military training. *Guide to Simulation-Based Disciplines: Advancing Our Computational Future*, 315-361

Bruzzone, A., Massei, M., Longo, F., Poggi, S., Agresta, M., Bartolucci, C. & Nicoletti, L. (2014a). Human behavior simulation for complex scenarios based on intelligent agents. In Proceedings of the 2014 Annual Simulation Symposium (pp. 1 10).

Bruzzone, A., Massei, M., Longo, F., Poggi, S., Agresta, M., Bartolucci, C., & Nicoletti, L. (2014b, April). Human behavior simulation for complex scenarios based on intelligent agents. In *Proceedings of the 2014 Annual Simulation Symposium* (pp. 1-10).

plants. Progress in Nuclear Energy, 128, 103446.

Bruzzone, A. G., Tremori, A., Tarone, F., & Madeo, F. (2011). Intelligent agents driving computer generated forces for simulating human behaviour in urban riots. *International Journal of Simulation and Process Modelling*,*6*(4), 308-316.

Cayirci, E., AlNaimi, R., & AlNabet, S. S. (2022, December). Computer assisted military experimentations. In 2022 Winter Simulation Conference (WSC) (pp. 1311-1324). IEEE.

Chaturvedi, S. K., Sekhar, R., Banerjee, S., & Kamal, H. (2019). Comparative review study of military and civilian unmanned aerial vehicles (UAVs). *INCAS bulletin*, *11*(3), 181-182.

Claverie, B., & Du Cluzel, F. (2022). "Cognitive warfare": The advent of the concept of "cognitics" in the field of warfare. Cognitive Warfare: the future of cognitive dominance, 2-1.\

Fang, W., Shunshan, F., Wenxuan, W., & Fuwang, L. (2010, October). Analysis of action mechanism of graphite bombs and reaction method of power system. In 2010 International Conference on Power System Technology (pp. 1-6). IEEE.

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, 2(1), 51-75.

Miętkiewicz, R. (2018). Unmanned surface vehicles in maritime critical infrastructure protection applications—LNG terminal in Świnoujście. *Maritime Technical Journal*, *213*(2), 43-51.

Hodicky, J., & Hernandez, A. S. (2021). Wargaming, Automation, and Military Experimentation to Quantitatively and Qualitatively Inform Decision-Making. Simulation and Wargaming, 123-156.

Hodický, J., Procházka, D., Baxa, F., Melichar, J., Krejčík, M., Křížek, P., ... & Drozd, J. (2020). Computer assisted wargame for military capability-based planning. Entropy, 22(8), 861.

Hodicky, J. (2017, July). Wargaming and Challenges in the Experimentation Domain. In International conference KNOWLEDGE-BASED ORGANIZATION (Vol. 23, No. 1, pp. 144-149).

Kontouras, Efstathios, Anthony Tzes, and Leonidas Dritsas. "Cyber-attack on a power plant using bias injected measurements." In 2017 American Control Conference (ACC), pp. 5507-5512. IEEE, 2017.

Wiseman, E., & Defence, R. (2014). Critical infrastructure protection and resilience literature survey: modeling and simulation. Defence Research and Development Canada.

Zhang, F., & Coble, J. B. (2020). Robust localized cyber-attack detection for key equipment in nuclear power