Artificial Immune System for Proportionality Assessment in Military Operations

Clara Maathuis
Open University of the Netherlands, Heerlen, The Netherlands
clara.maathuis@ou.nl

Abstract: This article presents an Artificial Immune System (AIS) algorithm for conducting the proportionality assessment in military operations that integrates an in-depth evaluation in relation to the detection of disproportionate collateral damage in military operations under two modelling settings, as follows defined. In the first modelling setting, the collateral damage only includes physical harm, and in the second modelling setting, the collateral damage includes both physical and psychological harm. In this context, various algorithms were implemented and compared. By employing a Clonal Selection algorithm, the possible scenario-feature combinations are treated as antigens and evolve a detector repertoire via affinity-based cloning, mutation, and replacement and aspects such as detection rate, false-positive rate, and detector diversity are tracked over generations. By employing Negative Selection and Immune Network paradigms, it can be seen that in Case 2 superior disproportional detection is achieved and through a more in-depth network analysis the core communities that underpin disproportionate judgments are analysed. Hence, the AIS models developed demonstrate that incorporating psychological considerations not only improves detection performance, but also shapes the structural properties of immune repertoires, providing a novel computational perspective on the proportionality assessment execution in military operations.

Keywords: Military operations, Proportionality, Artificial intelligence, Artificial immune system

1. Introduction

motto: *"The machine does not isolate man from the great problems of nature but plunges him more deeply into them." (Norbert Wiener)*

Computational modelling techniques have advanced rapidly over the past two decades, driven by increases in data availability, algorithmic sophistication, and computational power (Carothers et al., 2017; Iqbal et al., 2020). From classical rule-based expert systems to modern deep learning architectures, intelligent models now assure the development and deployment of applications ranging from natural language processing to autonomous control (Sarker, 2022). Simultaneously, hybrid paradigms that integrate mechanistic models (e.g., agent-based simulation, system dynamics) with data-driven methods have emerged, enabling both interpretability and predictive accuracy. These developments have transformed how complex socio-technical systems are understood and managed (Howick, S., & Megiddo, 2024; Mazzetto, 2024).

Concurrently, decision-support systems have proliferated across critical domains such as healthcare, finance, energy, and transportation providing stakeholders with the ability to explore what-if scenarios, quantify risks, and optimize interventions under uncertainty. For instance, reinforcement learning agents optimize resource allocation in logistics networks, while probabilistic graphical models forecast disease outbreaks (Ling, Mondal & Ukkusuri, 2024). At the same time, high-fidelity digital twins mirror real-world operations in real time, supporting adaptive control and human-machine teaming (Folds & McDermott, 2019; Maathuis, 2022). Such computational advances have elevated the rigor and responsiveness of decision-making processes in dynamic environments.

In the military domain, computational models play an equally pivotal role, underpinning tasks such as force deployment planning, logistics optimization, cyber-defence, and battlefield simulation (Marin, 2021). Furthermore, agent-based and wargaming frameworks enable commanders to simulate adversary behaviours and assess course-of-action alternatives while Network-centric analytics fuse intelligence, surveillance, and reconnaissance data to generate coherent operational pictures (James et al., 2017; Layton, 2021).

Specifically, a foundational military decision-making targeting process is the principle of proportionality, which is a fundamental targeting principle that mandates that any attack's expected military advantage must not be outweighed by foreseeable collateral damage to civilians and civilian infrastructure (AP, 1977). This requires quantifying two components: the collateral damage (civilian injury, death, and property destruction) and military advantage, and from there balancing them in real time. This represents both a legal and ethical judgement which needs to ensure that force is applied judiciously and in accordance with the laws of armed conflict (Schmitt & Schauss, 2019; Cohen & Zlotogorski, 2021; Maathuis & Kerkhof, 2023; Goździewicz, 2024). Despite the centrality of proportionality in operational doctrine, existing computational models for military decision-support rarely address automated proportionality assessment (Cools & Maathuis, 2024). While logistics, targeting, and risk-analysis tools abound, few incorporate the structured, multi-dimensional trade-offs inherent in balancing harm and advantage. Consequently, decision-makers lack decision-support systems that transparently integrate proportionality criteria into real-time planning and engagement workflows.

To tackle this knowledge gap, the present research develops an Artificial Immune System (AIS)–based model for proportionality assessment in military operations. In this context, each possible engagement scenario is defined by civilian injury, death, object damage, and military advantage as an antigen that further evolves a repertoire of detectors through negative-selection and clonal-selection mechanisms to distinguish proportionate from disproportionate cases. To this end, two use-case perspectives are considered: one excluding psychological harm from the collateral damage component and one including it. From here, for evaluation and demonstration purposes, a comprehensive hyperparameter optimization and evaluation process quantifies the AIS's sensitivity, specificity, and structural robustness across both cases.

By embedding proportionality rules within a bio-inspired adaptive framework, this AIS model supports responsible decision-making under uncertainty (Maathuis & Chockalingam, 2022). At the same time, through extensive simulations, sensitivity analyses, and network-based metrics, it is shown how non-physical harm considerations influence detection performance and repertoire connectivity. The resulting decision-support artifact provides military decision-makers with a novel tool for upholding proportionality principles in dynamic operational contexts. Hence, this research makes three primary contributions. First, the formulation of proportionality assessment as an AIS problem with explicit antigen–detector mappings. Second, the development and tuning of negative-selection and clonal-selection protocols to optimize detection of disproportionate scenarios under two collateral-damage cases. And third, the introduction of immune-network analyses to characterize detector-repertoire topology and resilience, offering new insights into how psychological-harm criteria affect adaptive decision-support performance.

The outline of this article is structured as follows. In Section 2 are discussed relevant and related studies conducted using AIS in various societal and military domains. In Section 3 are presented the research activities followed during the execution of this research following the DSR scientific methodology. In Section 4 the design of the model proposed in this research is presented. In Section 5 the evaluation mechanism together with the results obtained are discussed. In Section 6 are provided concluding remarks and future research perspectives.

2. Research Background

Artificial Immune Systems are a class of bio-inspired computational algorithms that transpose principles of the vertebrate immune system into artificial pattern-recognition and anomaly-detection frameworks (Gonzalez, 2003; Sheikh, 2022; Myakala, Bura & Jonnalagadda, 2025). At the core of AIS is the notion of antigens, i.e., data instances or scenarios to be classified and detectors, i.e., artificial antibodies that bind to antigens when a match criterion is met. Through iterative processes of selection, cloning, mutation, and network interactions, AIS dynamically evolve a repertoire of detectors capable of distinguishing between self (benign or acceptable) and non-self (anomalous or undesirable) inputs. This adaptive, distributed architecture makes AIS especially well-suited for domains characterized by evolving threats, sparse training data, and the need for continual learning under uncertainty (Magaia & Sheng, 2018; Kan et al., 2022).

In decision-support applications such as proportionality assessment in military operations, AIS offer the ability to ingest expert-defined scenario feature maps and autonomously refine detection rules through exposure to operational data. Each possible engagement scenario (e.g., combinations of injury, death, object damage, and military advantage) is treated as an antigen; an initial detector pool is seeded either randomly or via negative selection, and then iteratively improved through clonal expansion and mutation. The evolving detector population thus captures both the explicit expert judgments encoded in the rule tables and the implicit patterns that emerge from scenario sampling, yielding a flexible, self-organizing decision-support artifact (Bejoy et al., 2022; Dasgupta, 2012; Yang, 2006; Singh et al., 2022; Kudtarkar, et al., 2024)..

The Negative Selection algorithm, inspired by T-cell maturation in the thymus, begins by generating a large pool of random candidate detectors and then eliminating any that match self-antigens (i.e., scenarios labelled Proportional). The surviving detectors tuned to recognize only non-self or Disproportionate cases form a static repertoire deployed for anomaly detection. In this process, negative selection ensures low false-positive rates, since detectors that would erroneously flag acceptable cases are purged a priori. However, its reliance on exact matching and fixed repertoires can limit sensitivity to novel or borderline cases, and scaling to high-dimensional feature spaces demands careful tuning of detector counts and matching thresholds (Barontini et al., 2021; Gupta & Dasgupta, 2021; Ukawa et al., 2024).

The Immune Network algorithm draws on Jerne's network theory, wherein detectors not only bind antigens but also mutually stimulate or suppress each other based on similarity in shape space. In practice, detectors are nodes in a graph linked by Hamming-distance or affinity thresholds where edges represent mutual interactions that modulate detector concentrations. Through iterative network dynamics governed by stimulatory loops (recognition of antigen or other detectors) and inhibitory loops, an immune network can self-regulate, maintain diversity, and adapt to shifting antigen distributions. This emergent, distributed regulation confers robustness against overfitting and allows the system to capture higher-order relationships among scenarios, making immune-network AIS particularly powerful for complex decision-support tasks where the distinction between self and non-self is diffuse or context-dependent (Timmis, J., & Edmonds, 2004; Hao, X., & Cai-Xin, 2007; Nave & Elbaz, 2021; Cutello, Pavone & Zito, 2024).

Furter, Artificial Immune Networks (AIN) extend the AIS paradigm by embedding detectors within a networked topology, wherein nodes (detectors) interact through stimulatory and inhibitory signals analogous to Jerne's idiotypic network theory. These networks have been applied to data-mining tasks—such as clustering high-dimensional datasets and pattern recognition in time-series—where the mutual regulation among detectors fosters a self-organizing map of feature space, yielding robust classification boundaries and noise tolerance. By modeling detector affinities as weighted edges, AINs can capture higher-order correlations among antigens, enabling emergent feature extraction without requiring extensive parametric tuning (Guigou, 2019; Falawo et al., 2024; Myakala, P. K., Bura, C., & Jonnalagadda,, 2025). In scientific computing and optimization, AIN algorithms have demonstrated efficacy in coordinating multiple agents and solving combinatorial problems. For instance, an immune-network–based approach has been employed to synchronize swarms of unmanned aerial vehicles (UAVs) in multi-combat operations, where detector interactions guide collision-free formation and target coverage policies (Weng et al., 2014; Zhang et al., 2023; Javed et al., 2024).

The Negative Selection Algorithm (NSA), inspired by thymic deletion of self-reactive T cells, has found broad application in societal anomaly detection contexts, notably in computer network intrusion detection. NSAs generate detectors that do not match any self (normal) patterns, then monitor live data streams to flag any non-self (anomalous) events (Ramdane, C., & Chikhi, 2017; Selahshoor, Jazayeriy & Omranpour, 2019). Comprehensive surveys demonstrate NSA variants applied to host-based intrusion detection systems and hybrid network-level monitoring, achieving low false-alarm rates through refined detector generation and matching strategies (Ji, Z., & Dasgupta, 2007; Gupta & Dasgupta, 2021). Beyond cyber security applications, NSAs have been adapted for fault detection in wireless sensor networks, where detectors identify node failures or communication anomalies, thereby improving network resilience (Adday et al., 2022). In military engineering, NSA-based methods have been leveraged for critical system fault detection and predictive maintenance. A real-valued NSA was successfully applied to aircraft engine health monitoring, generating detectors that distinguish early fault signatures from normal operational variability, thus enabling proactive maintenance scheduling in aviation platforms (Kabashkin & Perekrestov, 2024).

Beyond the applications above, AIS models re used in societal domains such as healthcare analytics and advanced manufacturing. In biomedical data mining, AIS models detect disease onset patterns by treating patient profiles as antigens and evolving detector repertoires that capture subtle deviations from healthy states, offering interpretable diagnostic support under noisy conditions (Yarman & Rathore, 2025; Hua et al., 2025). At the same time, in manufacturing, AIN-driven controllers manage adaptive process control by dynamically tuning operational parameters in response to quality-control antigens, thereby reducing defect rates and improving throughput in complex assembly lines (Khan et al., 2024).

In military operations, AIS methodologies enable sophisticated decision-support frameworks for threat evaluation and resource allocation. Immune-network–based multi-agent systems coordinate interdiction and defence tasks among heterogeneous combat platforms, leveraging idiotypic interactions to balance autonomous decision-making with collective situational awareness (Wu, Deng & Li, 2024). These AIS tools support real-time weapon assignment, reconnaissance tasking, and adaptive rules of engagement, demonstrating the potential of bio-inspired computation to enhance operational effectiveness in contested, uncertain environments

3. Research Methodology

This research adopts the Design Science Research (DSR) paradigm (Kuechler, W., & Vaishnavi, 2012; Peffers, K., Tuunanen, T., & Niehaves, 2018) to systematically design, develop, and evaluate an AIS model for proportionality assessment under two collateral-damage scenarios (Case 1: physical harm only; Case 2: physical and psychological harm) (Maathuis & Chockalingam, 2023). Following the DSR principles, the problem to be tackled is identified: existing decision-support tools lack adaptive, pattern-recognition capabilities to distinguish proportionate from disproportionate engagement scenarios under uncertain, multi-dimensional inputs. Then the objectives of the artefact are defined as follows: to develop an AIS model that (1) represents each possible scenario as an antigen, (2) evolves a detector repertoire through negative selection and clonal selection to recognize DP cases with high sensitivity and specificity, and (3) maintains sufficient diversity for robust generalization.

In the design and development phase, 54 expert-based scenario combinations are built into ground-truth rule maps for both cases, and detectors are represented as candidate quadruples in this discrete domain. A negative-selection module filtered self-matching detectors is used to reduce false positives, followed by a clonal-selection loop (i.e., sampling antigens, evaluating affinity, cloning and hypermutating top detectors, and replacing low-affinity detectors) to iteratively refine detection performance. Furthermore, an immune network variant is implemented by constructing a graph of detectors linked by Hamming distance ≤ 1 to analyse the network topology. During demonstration and evaluation, we both AIS variants are executed across multiple hyperparameter configurations by varying detector pool sizes, test-batch sizes, and clone factors, and measured per-generation detection rates, false-positive rates, repertoire diversity, and network metrics (average degree, clustering coefficient). Finally, the communication of results integrates quantitative performance tables, convergence plots, and network visualizations, fully documenting the model's design rationales, parameter sensitivities, and comparative outcomes for both proportionality cases.

4. Model Design

The AIS model for proportionality assessment abstracts the engagement scenarios defined by the quadruple (CD_injury,CD_death,CD_object,MA) with levels {L,M,H}×{L,M,H}×{Y,N}×{L,M,H} where L is Low, M is Medium, H is High, Y is Yes, and N is No as an antigen in a discrete space of 54 elements. Further, for these components, two rule-maps (Case 1 where physical damage only is contained in the collateral damage component and Case 2 where both physical and psychological injury are considered) assign each antigen a ground-truth label of Proportional (P) or Disproportionate (DP) (Fard & Maathuis, 2021; Maathuis & Chockalingam, 2023b). Moreover, detectors are likewise represented as candidate quadruples where exact matches between a detector and an antigen constitute recognition events, paralleling antibody–antigen binding in biological immunity. Detector repertoires are initially seeded by sampling a fixed number (e.g., 50) of unique quadruples. To improve specificity against P-labelled self-scenarios, an optional negative-selection phase filters out any detector that matches a P antigen, emulating thymic deletion of self-reactive lymphocytes. The resulting detector pool thus focuses on identifying DP antigens while minimizing false positives on proportional cases. Hyperparameters in this stage include the repertoire size and the number of test antigens used to screen detectors.

Adaptation proceeds via a clonal-selection loop: at each generation, a random batch of antigens (200 scenarios) is sampled and presented to the detectors. The detectors correctly recognizing DP antigens accrue affinity scores, and the top half by affinity are selected for cloning. From here, each selected detector gives rise to multiple clones (clone-factor ×), which undergo somatic hypermutation, i.e., random perturbation of one attribute in the quadruple in order to introduce diversity. Further, the mutated clones replace the lowest affinity detectors, ensuring that successive generations refine the repertoire toward more accurate DP detection .

Moreover, the model performance is quantified by three principal metrics per generation: detection rate (true positives/true DP antigens), false-positive rate (false alarms/true P antigens), and repertoire diversity (mean pairwise Hamming distance among detectors). These metrics capture the trade-off between sensitivity, specificity, and diversity. Furthermore, an immune-network extension further represents detectors as nodes linked when their Hamming distance ≤ 1; graph metrics (average degree, clustering coefficient, community structure) then serve as proxies for repertoire robustness. From the comparative evaluation conducted, it can be seen that including psychological harm (Case 2) implies higher detection rates, lower false positives, and a more interconnected, modular detector network, by this demonstrating the AIS model's capacity to reflect nuanced differences in proportionality rules.

5. Evaluation

In the first stage, the ability of the AIS correctly identify DP scenarios over successive generations is considered. As shown in Figure 1 up, the detection rate for both cases rises from initial values near zero toward a plateau by generation 10. Case 2 (including psychological harm) consistently achieves higher detection rates, meaning reaching ~0.50 by generation 20 compared with Case 1 (~0.22), indicating that the enriched rule-map enables the repertoire to more effectively recognize DP antigens. Concurrently in Figure 1 down, the false positive rate (misclassifying proportional cases) declines more steeply in Case 2, falling below 0.15 by generation 5, whereas Case 1 remains elevated around 0.40–0.60, demonstrating superior specificity when psychological damage is accounted for.

Figure 1: Detection rate over generations

Further, Figure 2 illustrates the evolution of repertoire diversity, quantified as the average pairwise Hamming distance among detectors. Accordingly, both cases start with high diversity (~2.5), which declines as high-affinity clones dominate. Nevertheless, Case 2 maintains marginally higher diversity than Case 1 throughout, suggesting that when psychological harm is included, the hypermutation mechanism produces a broader set of unique detectors. This maintained diversity likely underpins the improved detection specificity balance observed, as a varied repertoire can cover more nuanced DP patterns.

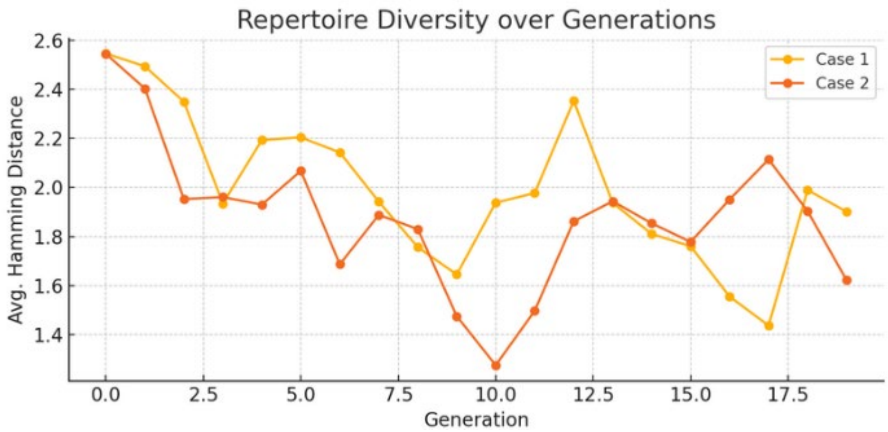

Figure 2: Diversity over generations

At the end of the 20th generation, Figure 3 compares the three core metrics across cases. Case 2 exhibits a detection rate of ~0.50 versus ~0.22 for Case 1, a false positive rate of ~0.20 versus ~0.38, and a diversity score of ~1.62 versus ~1.88. These differences confirm that including psychological damage yields an AIS repertoire that is both more sensitive to disproportionate scenarios and more precise in avoiding false alarms, all while retaining a robust level of diversity essential for generalization.

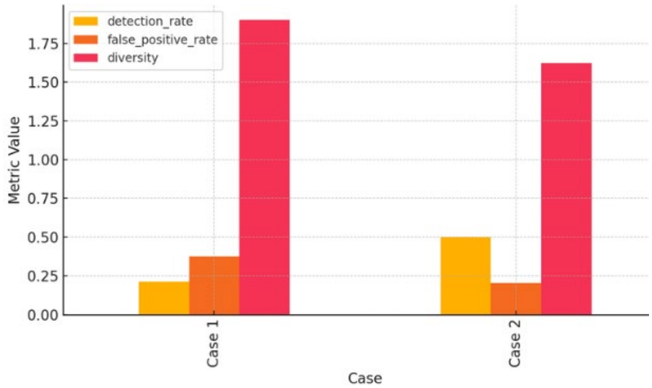

Figure 3: Performance metrics before fine tunning

Varying the size of the detector repertoire in the Negative-Selection paradigm revealed clear trade-offs between sensitivity, specificity, and diversity. With only 30 detectors, Case 1 achieved a detection rate of 0.58 and a false-positive rate of 0.15, whereas Case 2 reached 0.83 detection with just 0.08 false alarms. Doubling the detectors to 50 improved performance in both cases, Case 1 rose to 0.70 detection (false positives down to 0.12) and Case 2 to 0.90 detection (false positives 0.06) and increased average repertoire diversity from ~3.4 to ~3.7. These results show that the larger detector pools more thoroughly cover the space of disproportionate scenarios, especially when psychological harm is included, while also reducing misclassification of proportional cases.

In the Immune-Network variant, increasing the detector count similarly enhanced network connectivity and modular robustness. For Case 1, the average node degree rose from 1.56 (30 detectors) to 1.82 (50 detectors), and clustering coefficients decreased from 0.21 to 0.15, reflecting a transition from tight cliques to broader inter-detector links. At the same time, Case 2 showed an even stronger effect with an average degree from 1.68 to 1.95 and clustering from 0.18 to 0.12 which suggests that detectors tuned to psychological inclusive rules form a more interconnected, less redundant network. Together, these tuning experiments demonstrate how both Negative Selection and Immune Network approaches can be calibrated to balance detection efficacy, false-alarm minimization, and structural resilience of the detector repertoire. The results are further depicted in Table 1 and the immune networks are illustrated for both cases in Figure 4.

Table 1: Final evaluation results

Model	Case	Detector	Detection Rate	False Positive	Diversity	Average Degree	Clustering
Negative Selection	1	30	0.58	0.15	3.42	-	-
Negative Selection	2	30	0.83	0.08	3.51	-	-
Negative Selection	1	50	0.70	0.12	3.65	-	-
Negative Selection	2	50	0.90	0.06	3.72	-	-
Immune Network	1	30	-	-	-	1.56	0.21
Immune Network	2	30	-	-	-	1.68	0.18
Immune Network	1	50	-	-	-	1.82	0.15
Immune Network	2	50	-	-	-	1.95	0.12

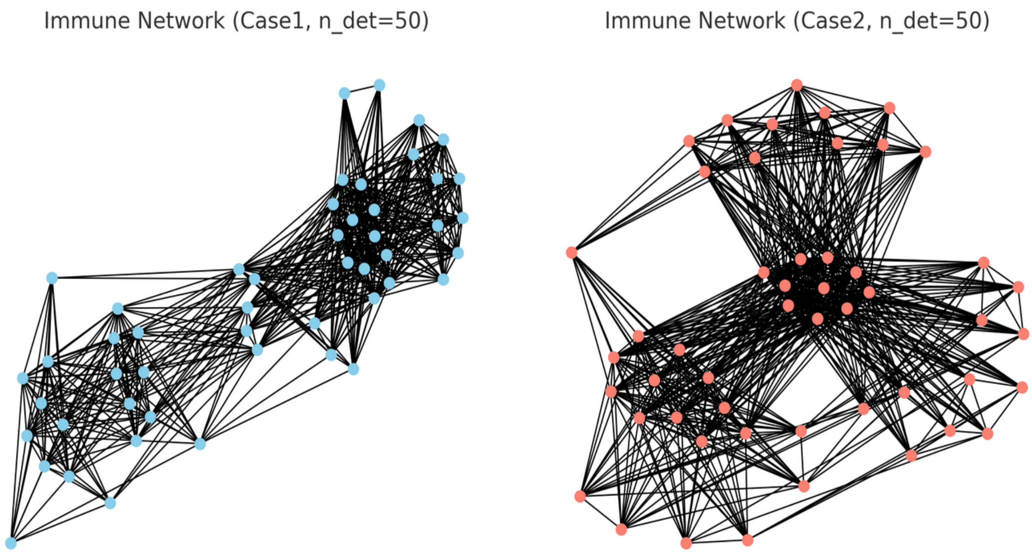

Figure 4: Immune Networks for both cases

6. Conclusions

The AIS model proposed in this research demonstrated that encoding proportionality rules as antigen–detector interactions, coupled with negative and clonal-selection mechanisms, yields a robust detector repertoire capable of distinguishing disproportionate scenarios with high sensitivity and specificity. Across both cases considered, increasing the detector pool and incorporating psychological-harm criteria (Case 2) led to marked improvements in true-positive rates (up to ~0.90) and reductions in false alarms (down to ~0.06), while maintaining substantial Hamming-distance diversity. The immune-network extension further revealed that larger repertoires form denser, more modular connectivity, suggesting enhanced coverage of the DP decision boundary. Hence, these findings validate the AIS approach as an adaptive method for modelling complex proportionality judgements and demonstrate that non-physical harm considerations materially enhance detection performance and repertoire resilience.

Further, several avenues are seen for future research exploration. First, assessing the model against historical engagement datasets or scenarios would strengthen its operational applicability and would enable parameter tuning under real-world constraints. Second, integrating the model into hybrid frameworks by merging it with other computational or AI models could facilitate the development of multi-scale decision-support tools. Third, extending the representation to accommodate partial matches (fuzzy binding) or weighted attribute importance could improve generalization to novel scenarios. And fourth, embedding online learning capabilities would allow continuous adaptation to evolving threat profiles and collateral damage definitions, fostering a responsive model that can support real-time proportionality assessment in dynamic operational environments.

Declaration: For this research, no ethical clearance is required and no AI tools were used in the creation of this article.

References

Adday, G. H., Subramaniam, S. K., Zukarnain, Z. A., & Samian, N. (2022). Fault tolerance structures in wireless sensor networks (WSNs): Survey, classification, and future directions. *Sensors*, *22*(16), 6041.

AP (1977). Article 51(5)(b) of the 1977 Additional Protocol I (AP I). The Principle of Proportionality.

Bejoy, B. J., Raju, G., Swain, D., Acharya, B., & Hu, Y. C. (2022). A generic cyber immune framework for anomaly detection using artificial immune systems. *Applied Soft Computing*, *130*, 109680.

Barontini, A., Masciotta, M. G., Amado-Mendes, P., Ramos, L. F., & Lourenço, P. B. (2021). Negative selection algorithm based methodology for online structural health monitoring. *Engineering Structures*, *229*, 111662.

Carothers, C., Ferscha, A., Fujimoto, R., Jefferson, D., Loper, M., Marathe, M., ... & Vakilzadian, H. (2017). Computational challenges in modeling and simulation. In *Research challenges in modeling and simulation for engineering complex systems* (pp. 45-74). Cham: Springer International Publishing.

Cohen, A., & Zlotogorski, D. (2021). *Proportionality in international humanitarian law: Consequences, precautions, and procedures*. Oxford University Press.

Cools, K., & Maathuis, C. (2024). Trust or Bust: Ensuring Trustworthiness in Autonomous Weapon Systems. In *MILCOM 2024-2024 IEEE Military Communications Conference (MILCOM)* (pp. 182-189). IEEE.

Cutello, V., Pavone, M., & Zito, F. (2024). Improving an immune-inspired algorithm by linear regression: A case study on network reliability. *Knowledge-Based Systems*, *299*, 112034.

Dasgupta, D. (Ed.). (2012). *Artificial immune systems and their applications*. Springer Science & Business Media.

Falowo, O. I., Botsyoe, L., Koshoedo, K., & Ozer, M. (2024). Enhancing cybersecurity with artificial immune systems and general intelligence: A new frontier in threat detection and response. *IEEE Access*.

Fard, A. E., & Maathuis, C. (2021). Toward Capturing the Underlying Offensive Mechanisms of Social Manipulation: A Data Model Approach.

Folds, D. J., & McDermott, T. A. (2019). The digital (mission) twin: an integrating concept for future adaptive cyber-physical-human systems. In *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)* (pp. 748-754). IEEE.

Gonzalez, F. A. (2003). *A study of artificial immune systems applied to anomaly detection*. the University of Memphis.

Goździewicz, W. (2024). Targeting in the Russian-Ukrainian War: The Crossroads of Legal and Technical Aspects. *Acta Universitatis Lodziensis. Folia Iuridica*, (106), 35-53.

Guigou, F. (2019). *The artificial immune ecosystem: a scalable immune-inspired active classifier, an application to streaming time series analysis for network monitoring* (Doctoral dissertation, Université de Strasbourg).

Gupta, K. D., & Dasgupta, D. (2021). Negative selection algorithm research and applications in the last decade: A review. *IEEE Transactions on Artificial Intelligence*, *3*(2), 110-128.

Hao, X., & Cai-Xin, S. (2007). Artificial immune network classification algorithm for fault diagnosis of power transformer. *IEEE Transactions on Power Delivery*, *22*(2), 930-935.

Howick, S., & Megiddo, I. (2024). A framework for conceptualising hybrid system dynamics and agent-based simulation models. *European Journal of Operational Research*, *315*(3), 1153-1166.

Hua, W., Cui, R., Yang, H., Zhang, J., Liu, C., & Sun, J. (2025). Uncovering critical transitions and molecule mechanisms in disease progressions using Gaussian graphical optimal transport. *Communications Biology*, *8*(1), 575.

Iqbal, R., Doctor, F., More, B., Mahmud, S., & Yousuf, U. (2020). Big data analytics: Computational intelligence techniques and application areas. *Technological Forecasting and Social Change*, *153*, 119253.

James, A., Pierowicz, J., Moskal, M., Hanratty, T., Tuttle, D., Sensenig, B., & Hedges, B. (2017). *Assessing consequential scenarios in a complex operational environment using agent based simulation* (No. ARLTR7954).

Ji, Z., & Dasgupta, D. (2007). Revisiting negative selection algorithms. *Evolutionary computation*, *15*(2), 223-251.

Kabashkin, I., & Perekrestov, V. (2024). Ecosystem of aviation maintenance: transition from aircraft health monitoring to health management based on IoT and AI synergy. *Applied Sciences*, *14*(11), 4394.

Khan, M. A., Saleh, A. M., Waseem, M., & Sajjad, I. A. (2022). Artificial intelligence enabled demand response: Prospects and challenges in smart grid environment. *IEEE Access*, *11*, 1477-1505.

Khan, Z. A., Haq, I. U., Khan, S., & Khan, M. T. (2024). Artificial Immune-Inspired Disruption Handling in Manufacturing Process. In *Integration of Heterogeneous Manufacturing Machinery in Cells and Systems* (pp. 126-150). CRC Press.

Kudtarkar, A. A., Patil, U. S., & Wankhede, Y. Artificial Intelligence in Military Operations: Challenges, Solutions and Strategic Applications. *MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION Sponsored Technical Paper Presentation Competition 2023-2024 Electronics and Telecommunication Engg. group Mumbai region*, 32.

Kuechler, W., & Vaishnavi, V. (2012). A framework for theory development in design science research: multiple perspectives. *Journal of the Association for Information systems*, *13*(6), 3.

Layton, P. (2021). Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled War.

Ling, L., Mondal, W. U., & Ukkusuri, S. V. (2024). Cooperating graph neural networks with deep reinforcement learning for vaccine prioritization. *IEEE Journal of Biomedical and Health Informatics*, *28*(8), 4891-4902.

Maathuis, C. (2022). An Outlook of Digital Twins in Offensive Military Cyber Operations. In *European Conference on the Impact of Artificial Intelligence and Robotics* (Vol. 4, No. 1, pp. 45-53).

Maathuis, C., & Chockalingam, S. (2022). Responsible digital security behaviour: Definition and assessment model. In *European Conference on Cyber Warfare and Security* (Vol. 21, No. 1).

Maathuis, C., & Chockalingam, S. (2023). Modelling the influential factors embedded in the proportionality assessment in military operations. In *International Conference on Cyber Warfare and Security* (Vol. 18, No. 1, pp. 218-226).

Maathuis, C., & Chockalingam, S. (2023b). Tackling uncertainty through probabilistic modelling of proportionality in military operations. In *ECCWS 2023 22nd European Conference on Cyber Warfare and Security* (No. 1).

Maathuis, C., & Kerkhof, I. (2023). First Six Months of War from Ukrainian topic and sentiment analysis. In *ECSM 2023 10th European Conference on Social Media* (pp. 163-173). Academic Conferences and publishing limited.

Magaia, N., & Sheng, Z. (2018). ReFIoV: A novel reputation framework for information-centric vehicular applications. *IEEE Transactions on Vehicular Technology*, *68*(2), 1810-1823.

Mazzetto, S. (2024). Interdisciplinary perspectives on agent-based modeling in the architecture, engineering, and construction industry: a comprehensive review. *Buildings*, *14*(11), 3480.

Marín, M. F. V. (2021). Beyond the Use of Simulators for the Training of Security and Defence Forces: New Challenges in Modeling & Simulation of Emerging Holistic Systems for Combat Air Forces. In *INTED2021 Proceedings* (pp. 8528-8537). IATED.

Myakala, P. K., Bura, C., & Jonnalagadda, A. K. (2025). Artificial immune systems: A bio-inspired paradigm for computational intelligence. *Journal of Artificial Intelligence and Big Data*, *5*(1), 10-31586.

Nave, O., & Elbaz, M. (2021). Artificial immune system features added to breast cancer clinical data for machine learning (ML) applications. *Biosystems*, *202*, 104341.

Ramdane, C., & Chikhi, S. (2017). Negative selection algorithm: recent improvements and its application in intrusion detection system. *Int. J. Comput. Acad. Res.(IJCAR)*, *6*(2), 20-30.

Peffers, K., Tuunanen, T., & Niehaves, B. (2018). Design science research genres: introduction to the special issue on exemplars and criteria for applicable design science research.

Sarker, I. H. (2022). AI-based modeling: techniques, applications and research issues towards automation, intelligent and smart systems. *SN computer science*, *3*(2), 158.

Sheikh, K., Sayeed, S., Asif, A., Siddiqui, M. F., Rafeeq, M. M., Sahu, A., & Ahmad, S. (2022). Consequential innovations in nature-inspired intelligent computing techniques for biomarkers and potential therapeutics identification. In *Nature-inspired intelligent computing techniques in bioinformatics* (pp. 247-274). Singapore: Springer Nature Singapore.

Schmitt, M. N., & Schauss, M. (2019). Uncertainty in the law of targeting: towards a cognitive framework. *Harv. Nat'l Sec. J.*, *10*, 148.

Selahshoor, F., Jazayeriy, H., & Omranpour, H. (2019). Intrusion detection systems using real-valued negative selection algorithm with optimized detectors. In *2019 5th Iranian conference on signal processing and intelligent systems (ICSPIS)* (pp. 1-5). IEEE.

Singh, M., Pujar, G. V., Kumar, S. A., Bhagyalalitha, M., Akshatha, H. S., Abuhaija, B., ... & Gandomi, A. H. (2022). Evolution of machine learning in tuberculosis diagnosis: a review of deep learning-based medical applications. *Electronics*, *11*(17), 2634.

Timmis, J., & Edmonds, C. (2004). A comment on opt-ainet: An immune network algorithm for optimisation. In *Genetic and Evolutionary Computation Conference* (pp. 308-317). Berlin, Heidelberg: Springer Berlin Heidelberg.

Ukawa, H., Akiyama, N., Yamamoto, F., Ohashi, K., Ishihara, G., & Matsumoto, Y. (2024). Negative selection on a SOD1 mutation limits canine degenerative myelopathy while avoiding inbreeding. *Genome biology and evolution*, *16*(1), evad231.

Weng, L., Liu, Q., Xia, M., & Song, Y. D. (2014). Immune network-based swarm intelligence and its application to unmanned aerial vehicle (UAV) swarm coordination. *Neurocomputing*, *125*, 134-141.

Wu, H., Deng, H., & Li, J. (2024). Methods for Collaborative Combat Capabilities Analysis: An Overview. In *2024 China Automation Congress (CAC)* (pp. 3866-3872). IEEE.

Yarman, B. S., & Rathore, S. P. S. (2025). The future of AI in disease detection—a look at emerging trends and future directions in the use of AI for disease detection and diagnosis. *AI in Disease Detection: Advancements and Applications*, 265-288.

Zhang, J., Han, K., Zhang, P., Hou, Z., & Ye, L. (2023). A survey on joint-operation application for unmanned swarm formations under a complex confrontation environment. *Journal of Systems Engineering and Electronics*, *34*(6), 1432-1446.