TDRD: A New Conceptual Model for Advanced Targeting Systems Using Artificial Intelligence Algorithms

Sandeep Bhattacharjee*

With the growth of hyper-active internet, the requirement of protection against hostile threats has become a matter of concern. In this article, an effort has been made to create a suggestive model based on Artificial Intelligence algorithms to understand the nature of calculated threat posed by potential threats and take necessary actions as and when deemed suitable. The suggestive model can be useful for policy-makers and concerned industries to consider more research effort unilaterally or collectively.

Keywords: *Advanced targeting system, artificial intelligence, human, model, technology*

Advanced Targeting Systems

There are systems for autonomous weapons and combat vehicles that can locate targets utilising sensor technologies created by the US Army and machine vision. The US Army is now evaluating ideas from various defence contractors in an effort to develop a completely automated ground vehicle that can engage in combat alongside human soldiers. The Advanced Targeting and Lethality Automated System is the name they give to their present design

* Mr Sandeep Bhattacharjee is Assistant Professor at Amity University, Kolkata.

ISSN 0976-1004 (print); 2583-7567 (online)

(ATLAS). The year 2017 saw the first demonstration of its sort and the most recent test of the ATLAS system. The Night Vision and Electronic Sensors Directorate of the Army are in charge of the ATLAS development project (NVESD).[1] They probably integrate their sensor technology into the project to support machine vision and enable reliable readings.

Use of Artificial Intelligence for advanced targeting system

By United States of America

The Integrated Sensor Architecture (ISA) has emerged as one of the possible architectures. This design enables information sharing between sensors and human-operated computers without the necessity for point-to-point hardware interconnection.[2]Every facet of the technology required to create ATLAS was discussed at a US Army industry day. Only a few of them actually mentioned AI or machine learning methods, despite the fact that each has its own potential uses for the technology. The following are the parts of the day that discussed artificial intelligence and machine learning:

1. Image Processing Topics, including AI/ML algorithms and automated image search.
2. Data Collection, including managing that data, organising it within databases, and using it to train ML algorithms.
3. Fire Control, or advanced targeting algorithms.

By China

The Chinese military's deployment of AI highlights the unpredictability and disruptive nature of the technology. Conventional combat may not have much of a role in today's battlefield as AI is changing the laws of the game, and China is utilising this to its maximum advantage. China is working in a grey area that other nations may find challenging to replicate because there is minimal regulation over the study and development of AI.[3]

Allen claims that China leads the world in several AI-related metrics, including the quantity of academic articles, patent applications and startup money. It is interesting to note that access to foreign financing and technological advancements play a major role in this dominance.

The AI sword can also cut in both directions. Since there is still much to learn about AI and machine learning, many wealthy nations are being cautious when implementing it, particularly in the military. China's aggressive pursuit of AI supremacy could have disastrous consequences because there isn't much time for testing for accuracy and dependability.

Latest Drone Market

The market for military drones was estimated to be worth US$ 13.4 billion in 2021 and is anticipated to grow at a CAGR of 11.7 per cent to reach US$ 26 billion by 2028. As more military organisations deploy drones to enforce the law globally, the sector is expanding. Additionally, growing government spending on military drones to boost the effectiveness of military operations raises demand for military drone production. Therefore, increased government spending on unmanned aircraft is driving the market for military drones.[4]

The worldwide military drone market is influenced by important aspects such as the expanding military budget, rising demand for better surveillance systems and technical advancements.

The Military Drone market has been dominated by a robust product range in both developed and emerging countries. The top companies that control the global military drone market include General Atomics Aeronautical Systems Inc. (GA-ASI) (US), Thales Group (France), Northrop Grumman Corporation (US), Israel Aerospace Industries Ltd (Israel), Elbit Systems Ltd (Israel), Lockheed Martin Corporation (US), AeroVironment Inc. (US) and Boeing (US).

Literature Review

History

Mateusz Pitkowski discussed the advancement of military technology in the 20th century that has reduced the quantity and complexity of jobs performed by military personnel while expanding the capabilities of machines and computers.[5]. However, the machines were never given the ability to make life-or-death decisions. The integration of airborne, land and marine systems is projected to substantially alter the current battlefield with the advent of highly advanced systems like Aegis Anti-Missile Ship Defense System. However, the current structure of international humanitarian law would undoubtedly face a significant challenge from these prospective weapons. The phrase 'dehumanization of combat' is not new in historical terms. The normal distance between the user and the weapon has been steadily growing ever since the arrows and crossbows were introduced. One essential component of the targeting process, however, is still present with the decision on human must still make the choice of when to fire or not the unique exception of the naval contact mines. Since the invention of artillery, aviation and other unidentified military machines, this phenomenon has continued to exist. The

US Air Force and Royal Air Force use UCAVs (Unnamed Combat Aerial Vehicles) with instances like Predator and Reaper drones working in manned systems, where the operator controls movement and aims from a distance.[6]

On the other hand, the shifting centers of power has made the countries realise the importance of asymmetric threats, rapidly developing conflict as a result of globalisation, terrorism, weapons proliferation, the growing East, and the rise of technology. In order to properly address these difficulties, the US military has made a similar adjustment as indicated by the research of Jesse McMurdo.[7] The new scenes of development include creation of a new battleground, cyberspace has assumed a differential status almost equivalent to conventional World Fighting II-style war of land, sea, air and space as fighting areas of arena. In airspace, a modern fighter plane is not very effective if its on-board systems and targeting network have been infiltrated, which suggests that cyberspace has arguably become the fundamental level upon which current war fighting capabilities are founded. For many years, the US Congress had shown interest in cruise missile defense.[8] A cruise missile's airframe, propulsion system, guidance system and weapons payload make it effectively an unmanned assault aircraft. They may have extremely sophisticated navigation and targeting systems, enabling them to maintain low, terra firma flight paths and attack with high precision as discussed by Hichkad and others.[9] CMs can be equipped with either conventional weapons or WMD and can be launched from a variety of platforms, including air, land or sea-based ones. The US Department of Defense has been working on numerous projects to strengthen defenses against an unpredictably dangerous cruise missile threat.[10]

Another significant study by F. Fernandez discussed cruise missile's airframe, propulsion system, guidance system and weapons payload which make it effective on an unmanned assault aircraft.[11] They may be equipped with extremely sophisticated navigation and targeting systems, which enables them to maintain low, terra firma flight paths and attack with high precision. CMs can also be equipped with either conventional weapons or WMD and can be launched from a variety of platforms, including air, land or sea-based ones.[12] Michael C. Horowitz in his paper examined how LAWS could affect two outcome areas: the development and deployment of systems, including arms races, and the stability of deterrence, including strategic stability, the risk of crisis instability, and wartime escalation.[13] It does this by drawing on classic security studies research and examples from military history. It focuses on issues using the possibility for enhanced operational speed and the potential for lessened human control over tactical decisions on the battlefield

as two features of LAWS. It also looks at how these problems intersect with the high level of uncertainty around prospective AI-based military weapons at the moment, both in terms of the possibilities and the programming transparency.[14]

Emily Crawford mentioned about types of remote warfare that are perfect for abiding by the principle of distinction.[15] Unmanned Aerial Vehicles (also known as UAVs or drones) are a type of technologically advanced weapons that can execute precision attacks, killing targets with a level of accuracy and certainty unsurpassed by earlier technology like missiles or bombs. In the world of cyberwarfare, carefully crafted software or computer code can target and disable extremely specific targets, ensuring that only those objectives are impacted by the attack leaving other systems unaffected. Brian Sanders et al. also pointed out the goal of integration of actuation systems based on smart materials for aircraft cruise and maneuver control.[16] Some relevant issues included evaluation of the increasing integration of AI in military systems with an eye towards the impact on crises stability, specifically how nations think about creating and deploying weapons, as well as when they are likely to go to war, and the possibilities for arms control. Cheng Lei et al. mentioned about the early discrete and independent individuals have now become extremely correlative and dependent on each another due to the ongoing popularisation and development of network applications.[17] The Internet of Everything not only fosters the development of a new social norm but also helps vital national infrastructure function effectively.

A recent research by Jing-lei Tan et al. discussed the availability of Software-defined networks (SDNs) that are prone to advanced persistent threats due to their centralised control features (APTs).[18] Moving target defense is constantly improving as a defensive tool. With current game models, it is challenging to accurately describe an MTD assault and defensive game and to accurately choose the defense timing to balance the benefits of MTD decision-making and SDN service quality. K. Zaffarano added that a flimsy defense against cyberattack could be more substantial on a static defense which could utilise proactive protective measures is still limited.[19] This is due to the fact that adaptable proactive defensive techniques like Moving Target Defense (MTD) have the potential to impede a network's ability to support the mission just as much as they have the capability to defend the network. Daesung Moon et al. addressed the attack processes using examples of APT attacks and argued the requirement for a comprehensive detection system.[20] In the present research, we suggested the Multi-Layer Defense System (MLDS), which can perform defence in depth by analysing data from the network, server, end-user, log,

etc., through the installation of agents at network appliances, servers and end-users.[21] In order to improve performance, MLDS recognises APT attacks from several layers. Additionally, MDLS lessens the harm when the system is subject to APT attacks.

Another enhanced concept on the examination of Ballistic Missile Defense System (BMDS) effectiveness has historically been imperfect, as discussed by T. Ender.[22] In fact, the BMDS battle management process entails keeping an eye on and managing the actions of a large number of interdependent participants (such as radar sensors, communications networks and interceptor missiles) in a process wherein a target moves from launch through sensor detection through intercept kill assessment. This article proposes a modelling and simulation (M&S) framework that supports architecture level analysis of the BMDS.[23] The key innovation is the application of neural network surrogate models, which are representations of other high- or medium-fidelity M&S tools, and can be executed rapidly with negligible loss in fidelity. Surrogate models were created of a BMDS analysis tool that included multi-sensor target tracking and fusion codes. Results will show the benefit of integrating M&S to architecture level analysis. Specific examples include sensitivity of operational level metrics to formation of an integration tracking picture, and the enabling architecture level decision making.[24]

As far as cyber physical systems are concerned, attacks could possibly include code injection, code reuse, and non-control data assaults. System defense against such attacks can be achieved using moving target defense (MTD) techniques including instruction set randomization (ISR), address space randomization (ASR), and data space randomization (DSR). MTD security method that offers predictable and dependable behaviour during normal operation and quick detection and reconfiguration upon detection of assaults, as discussed by Bradley Potteiger et al.[25] Research by Guilin Cai et al. on Moving Target Defense (MTD) has been put up as a paradigm-shifting idea to boost both the assault effort and the target system's security.[26] There are numerous MTD mechanisms that have been postulated among which some of them often run according to a few basic patterns which define how they function. Three main schools of thinking on MTD mechanisms were studied followed by defining and identifying three core running patterns used by these MTD processes. Five MTD mechanisms were run on these offered patterns, to create the three schools of thought. David Evans et al. suggested how MTD makes it considerably harder for an attacker to take advantage of a weak system by altering that system's features which may inconclusively give attackers a variable attack surface.[27] The defense system must be able

to incorporate dynamic changes which can possibly interfere with the operation of the exploit and not be affected by the learning of the attacker for existing defense mechanism. The domain of the future possible threats has been constantly expanding due to rapid changes in the military dynamics and capabilities which are due to advancement of indigenous technologies in many nations across the world. Adel Alshamrani discussed about the inclusion of private and corporate sectors as one of the measures to face such threats.[28] These classes of threats are also well-known as advanced persistent threats (APTs), which almost every nation and well-established organisation are aware of and would like to defend themselves against and develop long-term sustainable counter deterrence. Several cases of APT attacks had been studied and possible deployable monitoring and mitigating measures were also suggested for securing network systems.[29]

Ido Kilovaty indicated how large amounts of personal and non-personal data about Internet users are collected online and are being used increasingly in sophisticated ways for online political manipulation.[30] This illustrates a new pattern in the exploitation of data, where actors use cutting-edge artificial intelligence technologies to conduct data analytics, giving them easier access to people's cognition and potential future behaviour, as opposed to directly pursuing financial gain based on the face value of the data. Even though the idea of online manipulation has recently drawn some scholarly and policy interest, the ideal connection between cybersecurity law and online manipulation has not yet been thoroughly investigated. In other words, the relevance of connecting cybersecurity law to individual autonomy, privacy, and democracy has not yet been fully understood by regulators and courts. These facts raise questions about the survival potential of many enterprises to safeguard sensitive and mission-critical data from rivals, hostile states, and organised criminals. MTD, a cutting-edge and revolutionary method of cyber defence, is a promising solution to botnet identification and mitigation, as revealed by Massimiliano Albanese.[31] One of the prominent solutions to such threats could be modifying the network resource vulnerabilities, moving target defense, as a "game-changing" security solution for network warfare, thwarting the attackers' apparent assurance. In the research done by Tan Jing-lei et al.,[32] a unique optimal strategy selection technique had been developed using moving target defense based on Markov robust game to improve defence of unknown security threats.[33] The first step is to create a moving target defense model based on moving attack and exploration surfaces. This model combines Markov decision theory with robust game theory to exemplify how unknown prior information in the incomplete

information assumption is illustrated. Furthermore, it is demonstrated that there is an optimal approach for the Markov robust game. The defensive strategy is created by equivalently transforming the choice of optimal strategy into a non-linear programming issue. Further simulation and deduction of the suggested approach showed the viability of the created game model and effectiveness of the proposed approach.

Even if there have been significant research advancements in a number of MTD application domains, there are still a great deal of issues that need to be resolved. The ongoing development of new approaches and the interdisciplinarity of several disciplines also offer fresh perspectives on the conception and advancement of MTD study.

Jianjun Zheng and A.S. Namin pointed out the weakness of networking where network administrators face continuous difficult tasks as complexity and size of networks continue to increase.[34] Many network devices may not receive timely updates, leaving the network open to potential assaults. Additionally, because of the static nature of our current network infrastructure, attackers have the time to research the static configurations of the network and execute well-planned attacks whenever it is convenient, whereas defences must operate around-the-clock to protect the network. The motivation for MTD, an explanation of the key MTD concepts, ongoing research efforts into MTD and its implementation at each level of the network system, and potential future research opportunities provided by new technologies like Software-Defined Networking (SDN) and the Internet of Things are all covered in this article with a thorough survey of MTD and implementation strategies (IoT). Other capabilities such as faster data rates, lower latency, and ultra-reliability, 6G networks will elevate the digital capabilities provided by 5G to an entirely new level. To realise the potential of 6G, security of these systems is essential. The effective and widespread protection of 6G infrastructure and services is a crucial component of this demand, as discussed by Wissem Soussi et al.[35] In this article, the researchers see MTD as a vital component of proactive defense and go into detail about how it could be included into systems that are beyond 5G. In addition to this, discussion on future research prospects, pertinent research obstacles, and the standardizing perspective also features in the article.

Based on the discussion in the above-mentioned literature, there seems an urgent need to develop an effective model which can use the stated facts to develop an Artificial Intelligence powered, synchronized, fast attack structure for real-time targeting of hostiles which can be future potential threats individually or collectively with other potential hostile targets.

Secondary data has been used for collecting data related to the literature. Further, different models of artificial intelligence algorithms with high precision rates have also been modelled into the architectural layout of recognition types.

Data Analysis And Discussion

The data has been collected extensively using secondary research on various developments as recorded and stated by different published sources including journals and websites. The proposed model includes various stages with inherent algorithms as suggested by different researchers and have been put together to generate a coherent possibility of application and execution.

Model Development

(a) Stage A: Target Detection and Recognition (TDR)

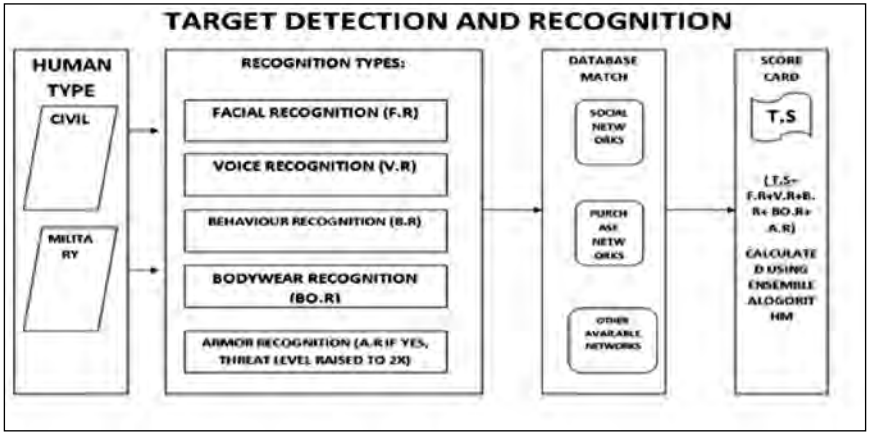

Figure 1 Architecture of TDR
Source: Author's analysis

Highly advanced sensors shall be needed to collect the data aided with satellite imagery for confirmation and analysis. Multiple sensors each for Facial recognition, Voice recognition, Behaviour recognition, Body wear recognition and Armor recognition can be used or a single advanced sensor can collect all such data together.

As seen in Figure 1, the TDR system consists of four essential parts namely:

i. Human Type

The human type has been classified into two groups namely the civil type with no association to any military, militia or in contract with some military of any nation and the military type with some or full association with the military, militia or in contract with some military of any nation.

ii. Recognition types
Under the recognition types, the system shall verify the human type classification with facial recognition, voice recognition, behaviour recognition, bodywear recognition, armor recognition with arms if any (using classification algorithms).

iii. Database Match
Once the recognition type is available, the social network, purchase network and any other available networks can be searched for with the primary key for such human identity. The data obtained can then be analysed using neural networks to verify the availability, feasibility, habits and other cognitive details which can determine scores obtained on a 10-point rating scale for each network.

iv. Score card
Individual scores calculated from each network can be assimilated and percentages can be calculated and categorised further under:
   a. High T.S score: Between (81% and above)
   b. Medium T.S score: Between (61%–80%)
   c. Low T.S score: Below 61%

(b) Stage B: Target Destruction and Evidence proof of destruction (TDEP)

See Figure 2, The TDEP model is related to the scorecard and the support structure available in the vicinity of the targeted object which is based on self artillery support, Joint support and self target support (when the other two support systems are not available).

The scorecard mainly includes target scores obtained and classified into either high score (H.S), medium score (M.S) and low score (L.S). After the classification is available, it can be forwarded to the support structure for implementation.

Depending upon the threshold, intensity and category of threat perceived, the higher scores can be communicated to the base support for artillery support, the medium scores can be communicated for joint support and those in the lowest can be self supported with self ammo.

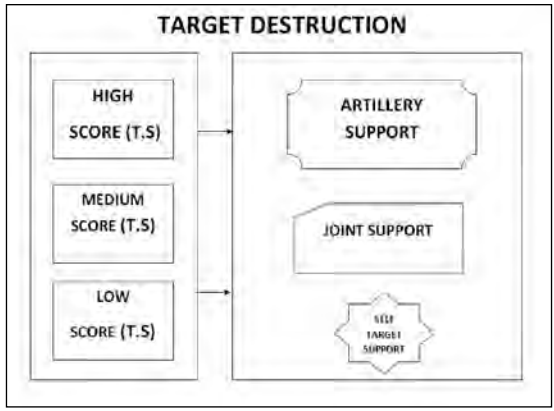

Figure 2 Architecture of TDEP
Source: Author's analysis

The features under consideration for possible human threat are: (to be collected by individual separate sensors or a combined sensor) (see Table 1).

1. Human face.
2. Human voice.
3. Human behaviour (personality, attitude).
4. Human body wear.
5. Human armor and arms if any (light weapons to heavy weapons).

Table 1 Proposed Algorithmic Selection

S. No.	Recognition Type	Algorithms	Usage
1.	Face Recognition	Naïve Bayes (Parametric), K- Nearest Neighbours (Non-parametric), Support Vector Machine (SVM), Deep Learning Convolutional Network (DLCNN) - Facebox.[36]	Classification of samples (parametric or Non-parametric)
2.	Voice Recognition	**1. Voice Recognition**: Hidden Markov models (HMM) and Dynamic Time Warping (DTW) Components used: **voiced sound, resonance, and articulation**.[37]	Based on: a. One is called **speaker dependent** and the other is **speaker independent**.

		Voice Recognition can work without NLP, but NLP cannot directly process audio inputs. **2. Natural language processing (NLP)** **Components of NLP** • Natural Language Understanding (NLU) extracting the metadata from content such as concepts, entities, keywords, emotion, relations, and semantic roles. ... • Natural Language Generation (NLG) Generating output in natural language of users.	b. Gender based Women (3 groups):_ **soprano,** **mezzo-soprano, and contralto**. Men (4 groups): **countertenor, tenor, baritone, and bass**
3.	Behaviour Recognition	Also known as Action Classification and Recognition Algorithm (see **Figure 3**)[38]	Performance comparison of different algorithms in different datasets and selecting the best algorithm with higher accuracy and fewer errors.
4.	Behaviour Recognition	Biosignal monitoring algorithms (see reference)[39]	The key issue that must be addressed is skin contact, which must be as excellent as possible in order to detect tiny voltages on the skin that occur throughout a cardiac cycle.
5.	Armor Recognition	SMCA-_-YOLOv5, multi-scale representation network (MS-RN) and shape-fixed Guided Anchor (SF-GA)[40]	Key issue to classify armors (light, medium, heavy), background, other hostiles[41]

Source: Author analysis

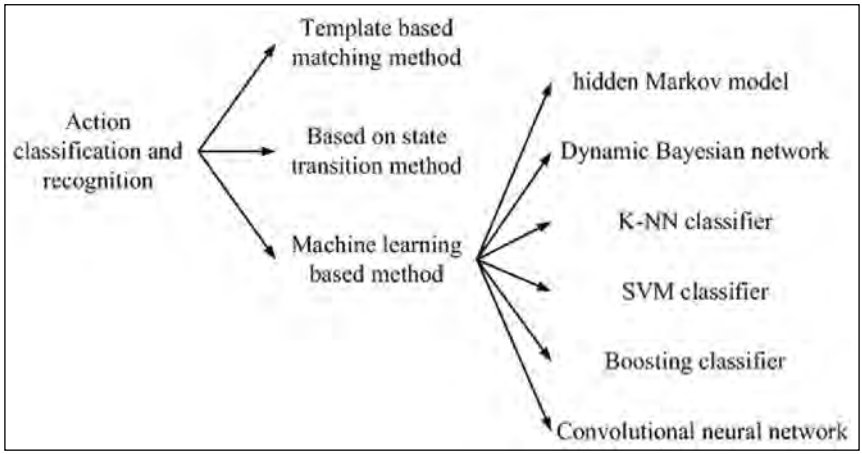

Figure 3 Action classification and recognition algorithms
Source: Author's analysis

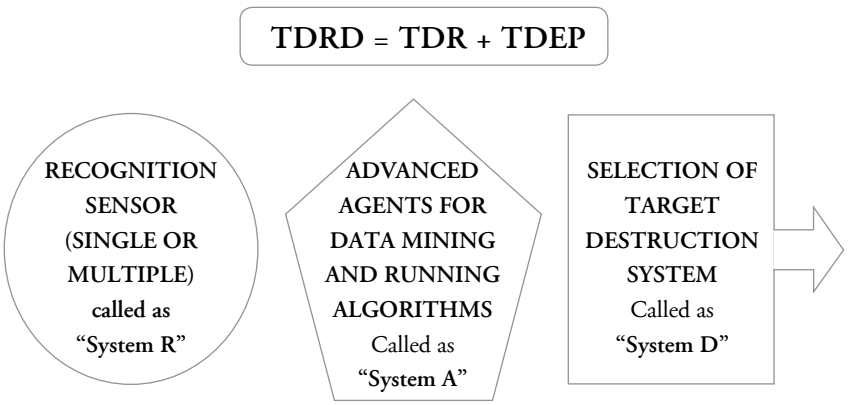

Figure 4 Interconnection of sub-systems of TDRD
Source: Author's analysis

Therefore, the proposed model could be named as TDRD, a combination of TDR (System R +System A) and TDEP (System D) (see Figure 4).

There are several advanced targeting systems used in various applications.[42] Here are a few examples:

a. *Laser-Guided Systems:* These systems use laser technology to target a specific location. The laser emits a beam that is reflected off the target,

and the reflected beam is detected by a sensor on the weapon or platform. The system then adjusts the weapon's aim to hit the target accurately.[43]

b. *GPS-Guided Systems:* These systems use Global Positioning System (GPS) technology to target a specific location. The GPS receiver on the weapon or platform receives signals from GPS satellites and calculates its position. The system then adjusts the weapon's aim to hit the target accurately.[44]
c. *Inertial Navigation Systems:* These systems use accelerometers and gyroscopes to track the weapon or platform's motion and calculate its position. The system can then adjust the weapon's aim to hit the target accurately, even if GPS is not available.[45]
d. *Image-Guided Systems:* These systems use cameras and sensors to detect and track the target. The system analyses the images and calculates the target's position and velocity. The system then adjusts the weapon's aim to hit the target accurately.[46]
e. *Radar-Guided Systems:* These systems use radar technology to detect and track the target. The system analyses the radar signals and calculates the target's position and velocity. The system then adjusts the weapon's aim to hit the target accurately.[47]

These targeting systems are used in various applications, such as military weapons, commercial aviation, and autonomous vehicles. Each system has its advantages and limitations, and the choice of the targeting system depends on the specific application's requirements.[48]

This TDRD system model can be mounted on UAVs (unmanned aerial vehicles), other aerial systems, ground systems, ground combat vehicles, sea-based systems that can purposefully determine the nature of threat posed by humans or humans occupied systems and neutralise such threats with precision.

Moreover, TDRD can send such data and information to the command station for analysis of threats and take other measures besides neutralising the effect of targeted humans or systems.

Conclusion

From the above literature and discussion on the proposed model development, we can conclude that there is an urgent need to develop fast Artificial intelligence algorithms integrated with each other to facilitate a unique super system that can determine the calculated threat posed by potential humans and systems and take necessary actions as and when deemed suitable. The above system can

be initiated as the base model of development for a real-time improved system that can aid Indian armed forces in their battle against hostiles both within and outside the Indian territories as needed for national security.

The proposed system can be further developed with the aid of further support needed in this domain.

Notes

1. J. Kovach and L. Sadler, *Integrated Sensor Architecture (ISA) Database/Media Storage Tool Software Package Documentation,* CCDC Army Research Laboratory, 2019.
2. Ibid.
3. M. Abadicio, 'Artificial Intelligence in the Chinese Military| Current Initiatives', *Emerj Artificial Intelligence Research,* 2019.
4. 'Unmanned Systems', Fortune Business Insights, available at https://www.fortunebusinessinsights.com/military-drone-market-102181.
5. Mateusz Piątkowski, 'Fully Autonomous Weapons Systems and the Principles of International Humanitarian Law', 5th International Conference of PhD Students and Young Researchers How Deep Is Your Law? Brexit. Technologies. Modern Conflicts Conference Papers, 27–28 April 2017, Vilnius University Faculty of Law, Vilnius, Lithuania, pp. 298–309, available at https://ssrn.com/abstract=3006230.
6. B. Sanders, R. Crowe and E. Garcia, 'Defense Advanced Research Projects Agency–Smart Materials and Structures Demonstration Program Overview', Journal of Intelligent Material Systems and Structures, Vol. 15, No. 4, 2004, pp. 227–33.
7. Jesse McMurdo, 'Cybersecurity Firms — Cyber Mercenaries?', 12 December 2014, available at https://ssrn.com/abstract=2556412 or http://dx.doi.org/10.2139/ssrn.2556412
8. Mateusz Piątkowski, 'Fully Autonomous Weapons Systems and the Principles of International Humanitarian Law', n. 5.
9. R.R. Hichkad and C. Bolkcom, 'Cruise Missile Defense', Library of Congress Washington DC Congressional Research Service, August 2004.
10. Ibid.
11. F. Fernandez, Director Defense Advanced Research Projects Agency, *Statement Before the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, United States Senate,* 1999.
12. Ibid.
13. Michael C. Horowitz, 'When Speed Kills: Autonomous Weapon Systems, Deterrence, and Stability', 2 May 2019, available at https://ssrn.com/abstract=3348356.
14. Ibid.
15. Emily Crawford, 'The Principle of Distinction and Remote Warfare', in Jens Ohlin (ed.), *Research Handbook on Remote Warfare,* 27 May 2016, Edward Elgar, UK,

2017, Sydney Law School Research Paper No. 16/43, available at https://ssrn.com/abstract=2785454.
16. B. Sanders, R. Crowe and E. Garcia, 'Defense advanced research projects agency–Smart materials and structures demonstration program overview', n. 6.
17. Ibid.
18. J.L. Tan, H.W. Zhang, H.Q. Zhang, C. Lei, H. Jin, B.W. Li and H. Hu, 'Optimal Timing Selection Approach to Moving Target Defense: A Flipit Attack-defense Game Model', *Security and Communication Networks, 2020.*
19. K. Zaffarano, J. Taylor and S. Hamilton, 'A Quantitative Framework for Moving Target Defense Effectiveness Evaluation', in *Proceedings of the Second ACM Workshop on Moving Target Defense,* October 2015, pp. 3–10.
20. D. Moon, H. Im, J. Lee and J. Park, 'MLDS: Multi-Layer Defense System for Preventing Advanced Persistent Threats', *Symmetry,* Vol. 6, No. 4, 2014, pp. 997–1010, available at http://dx.doi.org/10.3390/sym6040997.
21. Ibid.
22. T. Ender, R.F. Leurck, B. Weaver, P. Miceli, W.D. Blair, P. West and D. Mavris, 'Systems-of-Systems Analysis of Ballistic Missile Defense Architecture Effectiveness through Surrogate Modeling and Simulation, *IEEE Systems Journal,* Vol. 4, No. 2, 2010, pp. 156–66.
23. Ibid.
24 Ibid.
25. B. Potteiger, A. Dubey, F. Cai, X. Koutsoukos and Z. Zhang, 'Moving Target Defense for the Security and Resilience of Mixed Time and Event Triggered Cyber–Physical Systems', *Journal of Systems Architecture,* Vol. 125, 2022.
26. G. Cai, B. Wang, Y. Luo, S. Li and X. Wang, 'Characterizing the running patterns of moving target defense mechanisms', in *2016 18th International Conference on Advanced Communication Technology (ICACT),* January 2016, pp. 191–96).
27. D. Evans, A. Nguyen-Tuong and J. Knight, 'Effectiveness of Moving Target Defenses', *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats,* 2011, pp. 29–48.
28. A. Alshamrani, S. Myneni, A. Chowdhary and D. Huang, 'A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities', *IEEE Communications Surveys & Tutorials,* Vol. 21, No. 2, 2019, pp. 1851–77.
29 Ibid.
30. Ido Kilovaty, 'Legally Cognizable Manipulation (August 1, 2018)', *Berkeley Technology Law Journal,* Vol. 34, No. 2, 2019, available at https://ssrn.com/abstract=3224952.
31. M. Albanese, S. Jajodia and S. Venkatesan, 'Defending from Stealthy Botnets using Moving Target Defenses', *IEEE Security & Privacy,* Vol. 16, No. 1, 2018, pp. 92–97.

32. J.L. Tan, C. Lei, H.Q. Zhang and Y.Q. Cheng, 'Optimal Strategy Selection Approach to Moving Target Defense Based on Markov Robust Game', *Computers & Security,* Vol. 85, 2019, pp. 63–76.
33. C. Lei, H.Q. Zhang, J.L. Tan, Y.C. Zhang and X.H. Liu, 'Moving Target Defense Techniques: A Survey', *Security and Communication Networks,* 2018; B. Sanders, R. Crowe and E. Garcia, 'Defense Advanced Research Projects Agency–Smart Materials and Structures Demonstration Program Overview', *Journal of Intelligent Material Systems and Structures,* Vol. 15, No. 4, 2004, pp. 227–33.
34. J. Zheng and A.S. Namin, 'A Survey on the Moving Target Defense Strategies: An Architectural Perspective', *Journal of Computer Science and Technology,* Vol. 34, 2019, pp. 207–33.
35. W. Soussi, M. Christopoulou, G. Xilouris and G. Gür, 'Moving Target Defense as a Proactive Defense Element for Beyond 5G', *IEEE Communications Standards Magazine,* Vol. 5, No. 3, 2021, pp. 72–79.
36. Sanmoy Paul and Sameer Kumar Acharya, 'A Comparative Study on Facial Recognition Algorithms', *e-journal - First Pan IIT International Management Conference – 2018,* 21 December 2020, available at https://ssrn.com/abstract=3753064.
37. L. Muda, M. Begam and I. Elamvazuthi, 'Voice Recognition Algorithms Using Mel Frequency Cepstral Coefficient (MFCC) and Dynamic Time Warping (DTW) Techniques', *arXiv preprint arXiv:1003.4083.* voice recognition, 2010.
38. L. Wang, D.Q. Huynh and P. Koniusz, 'A Comparative Review of Recent Kinect-based Action Recognition Algorithms', *IEEE Transactions on Image Processing,* Vol. 29, 2019, pp. 15–28.
39. Tomasz Blachowicz, Guido Ehrmann and Andrea Ehrmann, 'Textile-based Sensors for Biosignal Detection and Monitoring', MDPI, available at https://www.mdpi.com/1424-8220/21/18/6042.
40. Jian Dai, Xu Zhao, Lian Peng Li and Xiao Fei Ma, 'GCD-YOLOv5: An Armored Target Recognition Algorithm in Complex Environments Based on Array Lidar', *IEEE Photonics Journal,* Vol. 14, No. 4, August 2022, available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9803045.
41. Fan-jie Meng, Xin-qing Wang, Fa-ming Shao, Dong Wang and Xiao-dong Hu, 'Fast-armored Target Detection Based on Multi-scale Representation and Guided Anchor', *Defence Technology,* Vol. 16, No. 4, August 2020, pp. 922–32, available at https://www.sciencedirect.com/science/article/pii/S221491471931044X.
42. Available at https://chat.openai.com/chat?__cf_chl_tk=Qs4m6_Bl5paLSS3RlANAtuEXEY5PQJXAQUEyL6fO14Q-1676367901-0-gaNycGzNGns
43. Ibid.
44. Ibid.
45. Ibid.
46. Ibid.
47. Ibid.
48. Ibid.