MBNA Publishing House Constanta 2025

Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

GAMEINT – A new paradigm in intelligence, with a focus on the field of video games

To cite this article: R. MOINESCU, C. RĂCUCIU, C.-S. OPRINA, Proceedings of the International Scientific Conference SEA-CONF 2025, pg. 7-16.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-25-001

GAMEINT – A new paradigm in intelligence, with a focus on the field of video games

Radu MOINESCU, Ciprian RĂCUCIU, Carmen-Silvia OPRINA

Military Technical Academy "*Ferdinand I*"
radu.moinescu@gmail.com

Abstract. This study introduces the innovative concept of Game Intelligence (GAMEINT), an emerging branch of intelligence that focuses on the exploitation of data generated by video games. This research explores the potential of video games as unconventional sources of intelligence, with applications ranging from the military to national security or electronic surveillance. Also, by analyzing in-depth data extracted from video games, including player behavior, social interactions, geographic location and preferences, behavioral patterns can be identified, risk assessments can be made, predictive models can be developed and scenarios can be anticipated, thus contributing to improving intelligence collection, analysis and interpretation capabilities. The study also examines the ethical and legal implications of using game data for intelligence purposes.

1. Introduction

Introduction

Video games have gone beyond their status as a simple form of entertainment, becoming complex platforms for social interactions, data collection and exploration of virtual worlds. This context aims to establish a new concept in the field of intelligence: Game Intelligence (GAMEINT). GAMEINT is an innovative approach that uses data generated by video games to obtain strategic information. By analyzing the behavior of players, their geographical locations, their interactions and preferences, GAMEINT can significantly contribute to the understanding of global dynamics and the development of advanced security strategies. This new paradigm offers a unique prism through which complex conflict scenarios can be explored and modeled, allowing intelligence analysts to identify behavioral patterns that can be extrapolated to the real world.

Unlike traditional intelligence sources, which often rely on fragmented and contextual data that require multiple sources to validate, GAMEINT enables a granular and systematic analysis of individual and collective actions in a rich and complex virtual environment. Each player action, from strategic to tactical decisions, can be decomposed and correlated with a multitude of variables, including the virtual context, mission objectives, simulated social and emotional pressures, as well as the player's individual characteristics (skills, preferences, cognitive style etc.). This granularity of data allows the identification of complex behavioral patterns, which can then be extrapolated to understand social and decision-making dynamics in real-world scenarios, with significant implications for different domains.

This study explores the potential of video games as unconventional sources of intelligence, analyzing how the data collected can be used for military, national security, or electronic surveillance purposes. It also discusses the key technologies underlying GAMEINT, as well as the ethical and legal implications of using game data.

2. Substantiation of the concept of GAMEINT

GAMEINT harnesses the potential of data generated within interactive virtual environments, particularly video games. The ability to model and simulate complex scenarios, including those with military and geopolitical implications, is a crucial aspect of GAMEINT. Combat simulators and strategy games provide a safe and controlled environment to test different strategies, tactics, and technologies, as well as to evaluate the effectiveness of different organizational and decision-making models. By analyzing the behaviors of players in these scenarios, intelligence analysts can identify strengths and weaknesses of different approaches, as well as potential vulnerabilities and risks.

2.1. Geolocation and the impact on electronic surveillance

Location-based games, such as Pokémon Go, Ingress, Jurassic World Alive or The Walking Dead: Our World, although the last mentioned is no longer active, facilitate the collection of precise information about players' locations in real time (Fig. 1). These platforms can provide detailed insight into users' behavior in the physical environment, and in combination with advanced geolocation technologies (GPS, Wi-Fi, Bluetooth), allow their routes to be traced. This capability is essential for identifying potential persons of interest, as it facilitates electronic monitoring of players' movements in/near areas of strategic interest, including government, military or industrial locations. Similar to the risks identified in the use of fitness apps [1] [2], the data generated by these games can reveal sensitive information.

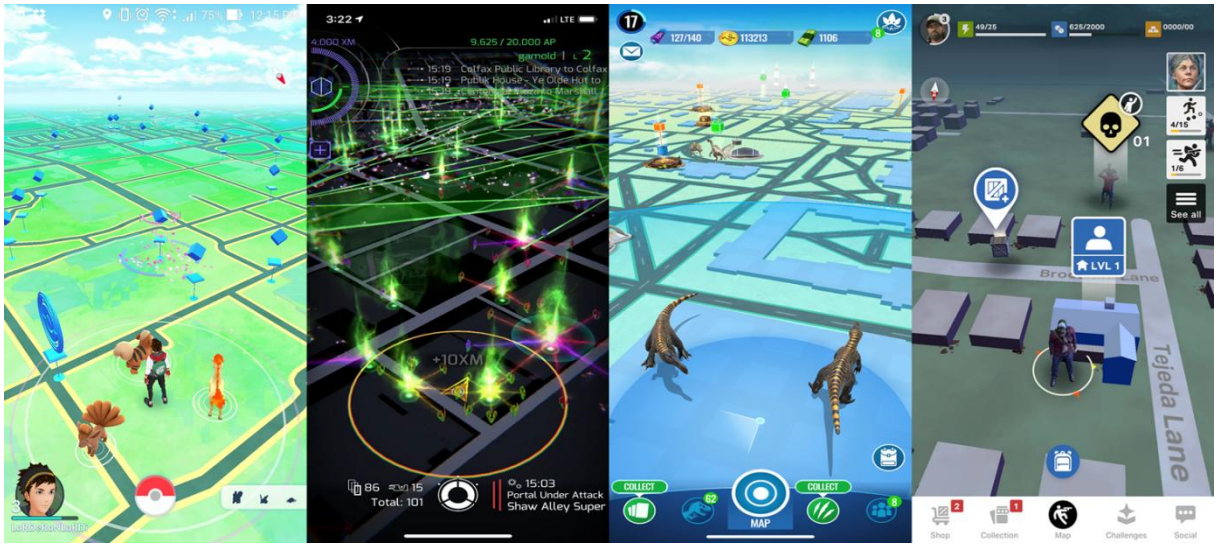

Fig. 1. Screenshots from Pokémon Go, Ingress, Jurassic World Alive and The Walking Dead: Our World

A relevant example is the game Ingress, which uses geolocation to place strategic objectives in locations around the world. In this case, interested entities can analyze the movement patterns and concentration of players in certain regions to understand mobility behaviors and economic or political activity in a given area. By analyzing frequently visited locations and interactions between players, hidden goals, possible locations of interest or even illegal activities can be identified. At the same time, in military conflicts, opponent targets can be located, facilitating hitting them with great accuracy/precision. [3]

In 2016, US security agencies, such as the NSA and the Department of Energy, expressed concerns that Pokémon Go players were being detected near sensitive locations, including military bases and nuclear laboratories. This phenomenon raised suspicions that the game could be exploited for covert intelligence gathering. [4] Although there was no concrete evidence that this game was being used for espionage, the incident highlighted the risks associated with location-based games and their potential for intelligence purposes.

2.2. Behavioral analysis: decisions, collaboration and conflicts

Massively multiplayer online (MMO) and social games provide an ideal environment for user behavioral analysis. By tracking players' decisions and actions, patterns of behavior, motivations, and possible hidden intentions can be identified.

An illustrative example is the use of World of Warcraft and other MMOs by intelligence agencies to monitor player interactions. According to documents leaked by Edward Snowden, the NSA and GCHQ infiltrated such games to gather information about potential terrorist activities and to identify persons of interest. The agencies suspected that extremist groups could use the virtual environment for communication and training [5].

By analyzing behavior in strategic games, analysts can also understand how individuals make decisions under pressure, allocate resources, or collaborate in teams. Such data is valuable for psychological profiling and risk assessment.

2.3. Player motivation and psychological profiling

The play styles and choices players make in various video games can reveal their motivations as well as their behavioral tendencies. For example, in role-playing games (RPGs), where players can choose to play as heroes or villains, they express their ideologies, values, and preferences that can provide significant information for risk assessment. Thus, data obtained from game behaviors can be used to build psychological profiles of players, helping analysts understand patterns of thought and reactions, which can be valuable in the context of analyzing extremist groups or persons of interest.

In multiplayer games, players can adopt different behaviors, from cooperation and collaboration to aggression and deception. The analysis of these behaviors can contribute to the assessment of an individual or group from a psychological perspective, helping to identify vulnerabilities or potential risks. Such a study can also be used to analyze and evaluate how individuals respond to pressure, challenges or conflicts, and this information can be extrapolated to anticipate reactions in real conflict or crisis scenarios. They are very useful in analyzing the psychological state of combatants in some military theaters or conflict zones, contributing to making operational decisions.

2.4. Simulating complex scenarios for strategic and tactical training

Tactical first-person shooters (FPS) games can be used by analysts to test and simulate different strategies and tactics of warfare, resource management, and combat under conditions of uncertainty. These games allow users to explore different tactical options and experiment with limited resources, and analyzing how players make decisions in these environments can provide valuable information for real-world war scenarios. These games can also be used to evaluate the effectiveness of combat approaches and identify the risks and vulnerabilities of various strategies [6] [7]. Data obtained from the analysis of these games can be useful for identifying optimal tactics in a real-world conflict and for testing techniques for combating enemies in a controlled environment.

Military operations in urban environments are extremely complex and challenging, involving not only military strategies but also interactions with the civilian population. These missions require constant adaptation to local conditions and a deep understanding of cultural dynamics. The dense and complex nature of urban terrain, coupled with the presence of non-combatants, creates a unique set of challenges. Tactical FPS games, particularly those designed to simulate urban settings, offer a valuable tool for exploring these complexities. For example, these games can be used to train soldiers in room clearing techniques, street fighting, and the difficult task of distinguishing between civilians and combatants in dynamic situations. Furthermore, analyzing player behavior in these virtual urban environments can provide researchers with valuable data on the effectiveness of different tactics and the potential consequences of various decisions. While acknowledging the limitations of game-based simulations, particularly in accurately modeling civilian behavior and the psychological pressures of real combat, tactical FPS games offer a cost-effective and accessible platform for studying and preparing for the unique challenges of urban warfare.

Military operations in urban environments are inherently complex and challenging, operating under conditions of extreme uncertainty. The enemy can be anywhere, hidden amongst the civilian population or concealed within the labyrinthine structures of the city. This pervasive uncertainty forces soldiers and commanders to make split-second decisions based on incomplete information, often with life-or-death consequences. The dense and complex nature of urban terrain, coupled with the ever-present threat of hidden enemies and the presence of non-combatants, creates a unique set of challenges. Tactical FPS games, particularly those designed to simulate urban settings, offer a valuable tool for exploring these complexities. For example, these games can be used to train soldiers in room clearing techniques, street fighting, and the difficult task of distinguishing between civilians and combatants in dynamic and unpredictable situations. By incorporating elements such as dynamic enemy Artificial Intelligence (AI) and randomized events, these games can replicate some of the uncertainty inherent in urban combat. Furthermore, analyzing player behavior in these virtual urban environments can provide researchers with valuable data on the effectiveness of different tactics and the potential consequences of various decisions made under pressure. While acknowledging the limitations of game-based simulations, particularly in accurately modeling civilian behavior and the psychological pressures of real combat, tactical FPS games offer a cost-effective and accessible platform for studying and preparing for the unique and uncertain challenges of urban warfare.

2.5. Integrating gaming platforms into intelligence analysis

Gaming platforms such as Steam, PlayStation Network and Xbox Live collect a significant amount of data about users' behaviors, preferences and gaming history. These platforms provide access to a vast amount of information that can be used to profile users, track online activities and identify patterns of behavior. For example, by analyzing game frequency, player interactions and favorite games, interested entities can obtain information about terrorist activities or the formation of terrorist networks that may be involved in online games.

Furthermore, certain games and platforms have already been the subject of controversies over the use of data for national security purposes, such as Riot Games and its ties to Tencent, a Chinese conglomerate that, according to some allegations, could use user data for government purposes. [8] [9] These platforms are thus valuable sources of information for analyzing user behavior and detecting global threats.

3. Technologies used in GAMEINT

GAMEINT relies on a sophisticated set of advanced technologies to collect, analyze and interpret data obtained from virtual environments, especially from video games. These technologies allow the extraction of essential information from the behaviors, interactions and choices of players, thus facilitating the analysis of complex scenarios for intelligence purposes. Within GAMEINT, emerging technologies that play a crucial role include AI, Machine Learning (ML), Natural Language Processing (NLP), Big Data analytics, Augmented Reality (AR) and Virtual Reality (VR), as well as visual image recognition.

3.1. Artificial Intelligence and Machine Learning

AI plays a central role in the data collection and analysis process within GAMEINT. ML algorithms are used to identify patterns and anomalies in player behavior, based on data collected from their interactions in video games. These technologies allow for massive data analysis and extracting insights from player behavior in real time, without requiring direct human intervention.

Furthermore, by applying ML algorithms, GAMEINT can create predictive-behavioral models that can anticipate players' decisions and choices based on the game's contextual variables.

3.2. Big Data Analysis

One of the fundamental pillars of GAMEINT is the use of Big Data analysis technologies. The volume, diversity and complexity of data generated in online gaming environments are considerable,

and their processing requires advanced data storage, management and analysis solutions. ML algorithms and NLP techniques are used to extract valuable information from data streams generated by players. In this context, Big Data allows the detection of behavioral patterns, the identification of emerging trends, the evaluation of tactics and strategies used by groups of players and, thus, the extraction of useful information for intelligence or strategic planning purposes. For example, the analysis of player behavior can provide relevant data for predicting their movements in a military conflict or in assessing the risks associated with specific operations.

3.3. Natural Language Processing

Another key technology area for GAMEINT is NLP. This technology is used to analyze and understand verbal and written communications of players, as well as to identify meanings, intentions and emotions in their interactions. In video games, players can interact not only through direct actions, but also through text messages, chats or voice, and NLP allows the processing and analysis of these interactions.

By using NLP, GAMEINT can detect signs of aggressive behavior, incitement to violence or even radicalization. For example, NLP algorithms can analyze written messages in games to identify the use of extreme language, signs of manipulation of other players or speeches that may indicate extremist intentions. NLP technologies can also be applied to analyze communications between players and assess the level of collaboration or conflict between them, providing valuable information for risk assessment and prevention of possible threats.

3.4. Augmented and Virtual Reality

AR and VR are emerging technologies that play an increasingly important role in GAMEINT, providing an immersive experience that can facilitate the simulation of conflict scenarios, military strategies, or psychological interactions. AR and VR are used to create virtual environments in which player behaviors and decisions can be studied in ways that mimic reality. These technologies can be used to analyze player reactions under stress, simulate combat scenarios, or evaluate the effectiveness of strategies and tactics. In the military, VR can be used to create simulations of dangerous or complex environments in which player behaviors can be observed and analyzed. For example, in combat simulations, analysts can study player reactions to attacks, security tests, or infiltration scenarios.

GAMEINT leverages AR to assess security risks in both physical and virtual environments by integrating real-world data with game elements. Unlike VR, which simulates entirely virtual environments, AR enhances real-world training. For counter-terrorism forces, AR overlays virtual threats, targets, and tactical information onto real locations, creating highly realistic training scenarios. For example, AR can simulate a hostage situation within a real building, projecting virtual adversaries and hostages. Trainees can then practice room clearing and hostage rescue protocols in a realistic context, with the AR system tracking performance and providing feedback. This integration of real and simulated elements improves training effectiveness and better prepares counter-terrorism units for complex challenges.

3.5. Visual analysis and image recognition technologies

In GAMEINT, visual analytics and image recognition technologies are used to examine visual elements in video games, which can include maps, terrain configurations, player movement patterns, and their behaviors in visual interactions. These technologies can be used to identify movement patterns, tactical strategies, and changes in player behaviors, especially in tactical FPS games.

Image recognition technologies can help analyze video game interactions, especially in games that involve navigating complex environments or visual conflicts. Also, by comparing visual behaviors and player movements with those of real-world risk groups, analysts can identify connections between virtual behaviors and predict their intentions in conflict scenarios.

4. Ethical and legal implications

The use of video game data for intelligence purposes raises a number of significant ethical and legal implications. The collection and analysis of players' personal data, even in the virtual environment, must respect fundamental data protection principles, such as informed consent, transparency and proportionality.

4.1. Privacy and data protection

Data collected from games can reveal sensitive information about players, including political preferences, sexual orientation, religious beliefs, or emotional state. It is crucial to ensure the confidentiality of this data and prevent its misuse or discriminatory use. Data protection regulations, such as the GDPR in the European Union, must be strictly adhered to.

4.2. Electronic surveillance and individual freedoms

The use of game data for electronic surveillance purposes can infringe on individual freedoms, privacy and the right to privacy. Monitoring players, even in a virtual environment, can create a sense of intrusion and limit freedom of expression and association. It is essential to set clear limits and control mechanisms to prevent abuse and protect the fundamental rights of players.

4.3. Responsibility and control

It is important to clearly define the responsibilities of the different parties involved in the collection and use of game data, including game developers and gaming platforms. Effective control mechanisms must be in place to ensure that data is used legally and ethically, and to prevent unauthorized access or misuse.

5. Simulation of GAMEINT data collection through game theory

To integrate elements of game theory into the analysis of data generated by location-based mobile games (such as Pokémon GO, Ingress, or Jurassic World Alive), we can use specific strategic game models and rational choice theory.

5.1. Defining players and strategies

Player 1 (P1) – The application user, who may have varying levels of technical skills to protect their data. He moves naturally, with daily habits and routines. It can modify routes and behavior that can reduce its profiling.

Player 2 (P2) – The application developer, who wants to collect data without raising suspicion and maximize the app's usage time. He analyzes and evaluates the data collected from P1 in order to create its profile.

P1 has the following data protection strategies available:

- S_1: *Passive attitude and lack of initiative*. P1 does not take any action, tacitly accepting the terms and conditions of the application. He continues his usual daily routine and does not use any protection mechanisms;
- S_2: *Cautious and reactive attitude*. P1 reads the terms and conditions of the application and tries to understand the implications for his personal data. He takes some basic precautions, such as adjusting privacy settings within the application and being mindful of the information he shares. He might also use some simple protection mechanisms, like avoiding sharing highly sensitive information. He is aware of the potential risks but doesn't employ advanced techniques (disables GPS when not using the app, VPN, permission restrictions);
- S_3: *Active and proactive attitude*. P1 carefully analyzes the terms and conditions of the application, assumes responsibility for the protection of personal data and takes measures to protect its information. He uses advanced techniques to make his profiling more difficult and

incorporate data protection mechanisms (GPS spoofing, emulator, VPN, device anonymization);

- S_4: *Uninstall/remove the application*.

P2 can use a variety of methods to perform a profile of P1:

- D_1: *Maximize data gathering*. Given P1's inaction, P2 can collect extensive data through various app functionalities, including usage patterns, location data, contact lists, and any other information the app requests access to. Profiling P1 is straightforward due to the readily available and unfiltered data. This passive approach by P1 presents the least resistance to P2's data collection efforts;
- D_2: *Cautious data gathering to minimize suspicion*. Introducing persuasion mechanisms to keep the user active. P2 must balance data collection with maintaining P1's engagement. While P1 is taking some precautions, they are not comprehensive. P2 can use in-app rewards, personalized content, or gamified features to subtly encourage continued usage and data sharing. A/B testing different engagement strategies can help optimize data collection without raising P1's suspicion. P2 might focus on collecting less sensitive data initially, gradually requesting more permissions as P1 becomes more comfortable with the app. Carefully crafted privacy settings and terms of service can also downplay the extent of data collection. The goal is to make P1 feel in control while still maximizing the data P2 can acquire;
- D_3: *Indirect data collection, accompanied by their correlation with information from alternative sources*. P2 faces significant challenges. P1's advanced techniques and data protection mechanisms make direct data collection difficult. P2's strategy must involve more sophisticated techniques, such as differential privacy, federated learning (if applicable), or potentially even exploring publicly available data to correlate with limited data gathered from P1. Profiling becomes significantly harder and less accurate. P2 might focus on collecting metadata or aggregated statistics rather than individual user data;
- D_4: *P1 profiling is not possible*. If the application is uninstalled/removed, P2 loses the data collection channel. P2's only recourse is to try and attract P1 back to the app with new features or incentives, hoping they will be less vigilant about data protection upon their return. This becomes a customer acquisition challenge for P2.

Let S be the set of strategies for P1:

$$S = \{S_1, S_2, S_3, S_4\}$$

We represent the probability that P1 chooses a certain strategy by a probability vector:

$$p = (p_1, p_2, p_3, p_4), \text{ were } \sum_{i=1}^{4} p_i = 1, p_i \geq 0$$

Let D be the set of strategies for P2:

$$D = \{D_1, D_2, D_3, D_4\}$$

Analogously, the choice probabilities of P2's strategies are:

$$q = (q_1, q_2, q_3, q_4), \text{ were } \sum_{i=1}^{4} q_j = 1, q_j \geq 0$$

5.2. Payoff functions

Let U_1 and U_2 be the utility functions for P1 and P2.

The user's utility function is based on the loss of privacy. The cost function can be defined as follows:

$$U_1(S_i, D_j) = -C(S_i, D_j)$$

where $C(S_i, D_j)$ represents the exposure level, defined by a matrix:

$$C = \begin{bmatrix} 10 & 7 & 5 & 0 \\ 7 & 5 & 3 & 0 \\ 5 & 3 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Thus, the user minimizes his cost:

$$\min_{S_i} U_1 (S_i, D_j)$$

The utility function of P2 reflects the value of the collected data:

$$U_2(S_i, D_j) = G(S_i, D_j) - R(S_i, D_j)$$

were $G(S_i, D_j)$ is the gain obtained from the data, and $R(S_i, D_j)$ it is a risk of penalties/suspicions. Expressed in a matrix:

$$G = \begin{bmatrix} 10 & 7 & 3 & 0 \\ 7 & 5 & 3 & 0 \\ 3 & 3 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

The application developer maximizes his profit:

$$\max_{D_j} U_2\left(S_i, D_j\right)$$

5.3. Feasibility constraints

Players must choose valid strategies, which requires:

$$\sum_{i=1}^{4} p_i = 1, \sum_{j=1}^{4} q_j = 1, p_i, q_j \geq 0$$

In addition:

$$G(S_i, D_j) \geq R(S_i, D_j), \forall (i, j) \Rightarrow \text{P2 must maintain profitability.}$$

5.4. Optimal Strategies

P1's optimal strategy:

$$S_1^* = \arg\min_{S_i} U_1(S_i, D_j)$$

P2's optimal strategy:

$$D_2^* = \arg\max_{D_j} U_2(S_i, D_j)$$

From the payoff matrix, it is observed that P1 minimizes the loss through S_4 (Uninstall/remove the application) or S_3 (Active and proactive attitude), and P2 maximizes it through D_1 (Maximize data gathering) if P1 is passive and D_2 (Cautious data gathering to minimize suspicion) if P1 is cautious.

5.5. Nash equilibrium

A Nash equilibrium is a pair of strategies (S^*, D^*) such that:

$$U_1(S^*, D) \leq U_1(S^*, D^*), \forall D$$
$$U_2(S, D^*) \geq U_2(S^*, D^*), \forall S$$

Identified Nash equilibria:

- $(S_2, D_2) \rightarrow$ the user is cautious, and the developer collects data carefully;
- $(S_3, D_3) \rightarrow$ the user protects their data, and the developer uses alternative sources;
- $(S_4, D_4) \rightarrow$ the user uninstalls, and the developer it's not able to collect data.

5.6. Game classification

Game typology:

- Non-cooperative game → each player maximizes his own utility;
- Non-zero-sum game → one player's loss is not always equal to the other's gain;
- Dynamic game (Follower-Leader) → P1 makes the move, and P2 reacts;
- Imperfect information game → the user does not know exactly how much information is being collected.

Mathematical proof → a non-zero-sum game satisfies the condition:

$$\sum_{i,j} U_1\left(S_i, D_j\right) + U_2\left(S_i, D_j\right) \neq 0 \text{ for all } (i, j)$$

Verification on the case (S_2, D_2)

$$U_1(S_2, D_2) + U_2(S_2, D_2) = -5 + 5 = 0$$

but in other cases, the sum is different from 0, so it is not a zero-sum game.

"*Follower-Leader*" type game → P1 acts first, and P2 reacts. The normal form is:

$$\max_{D} U_2\,(S, D) \text{ s.t. } S = \arg\min U_1\,(S, D)$$

Thus, the game can be modeled as a Stackelberg Game with P1 the leader and P2 the follower.

6. Conclusions

GAMEINT represents a new paradigm in intelligence, providing unique insights into human behavior and social dynamics through the analysis of data generated by video games. This innovative approach has significant potential for improving intelligence data collection, analysis, and interpretation capabilities, with applications in diverse domains, from military and national security, to electronic surveillance.

However, the use of game data for intelligence purposes raises a number of ethical and legal challenges that need to be addressed seriously in order to avoid violating citizens' rights and freedoms. It is essential to establish a clear legal and ethical framework to regulate the collection, analysis and use of game data, ensuring respect for the fundamental rights of gamers and preventing abuses.

Employing game theory, we characterize GAMEINT as a non-cooperative, dynamic Stackelberg game with imperfect information, thereby modeling the strategic interaction between users of the application and its developer.

Future research should focus on developing rigorous methodologies for game data analysis, exploring the potential of GAMEINT in different application areas, and analyzing the ethical and legal implications of this new paradigm in intelligence. It is also important to promote an open dialogue between researchers, policymakers, game developers and gamers to ensure that GAMEINT is used responsibly and for the benefit of society.

References

[1] Alex Hern – *Fitness tracking app Strava gives away location of secret US army bases*, January 28, 2018, web resource: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases, accessed on February 1, 2025

[2] Alex Hern – *Strava suggests military users 'opt out' of heatmap as row deepens*, The Guardian, January 29, 2018, web resource: https://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban, accessed on February 1, 2025

[3] Hunter Stoll – *Smart Devices: A Necessary Evil for Military Operations?*, Georgetown Security Studies Review, May 4, 2021, web resource: https://georgetownsecuritystudiesreview.org/2021/05/04/smart-devices-a-necessary-evil-for-military-operations/, accessed on February 1, 2025

[4] Zach Dorfman – *The Great Pokémon Go Spy Panic*, Foreign Policy, November 29, 2024, web resource: https://foreignpolicy.com/2024/11/29/pokemongo-cia-nsa-intelligence-spying/, accessed on February 1, 2025

[5] Paul Tassi – *New Snowden Leak Reveals The NSA Planted Agents Inside 'World of Warcraft'*, Forbes, December 09, 2013, web resource: https://www.forbes.com/sites/insertcoin/2013/12/09/new-snowden-leak-reveals-the-nsa-planted-agents-inside-world-of-warcraft/, accessed on February 1, 2025

[6] Evan Beebe – *5 Times the US Military Has Used Video Games for Training and Readiness*, Institute for Defense & Government Advancement (IDGA), October 21, 2024, web resource: https://www.idga.org/command-and-control/articles/5-times-us-military-used-video-games-for-training-and-readiness, accessed on February 1, 2025

[7] Scott Kuhn – *Soldiers maintain readiness playing video games*, US Army, April 29, 2020, web resource: https://www.army.mil/article/235085/soldiers_maintain_readiness_playing_video_games, accessed on February 1, 2025

[8] Matt Kim – *Tencent Designated as a Chinese Military Company by US*, IGN, January 7, 2025, web resource: https://www.ign.com/articles/tencent-designated-as-a-chinese-military-company-by-us?link_source=ta_first_comment&taid=677dd198ce05110001e523f3, accessed on February 1, 2025

[9] Bloomberg News – *Tencent Shares Decline After US Adds Company to Chinese Military Blacklist*, Bloomberg, January 7, 2025, web resource https://www.bloomberg.com/news/articles/2025-01-06/us-adds-tencent-to-chinese-military-blacklist-shares-decline, accessed on February 1, 2025