New Trends in Psychology

Thinking Traps: How High-Performance Information Systems Correct Cognitive Biases in Decision-Making

Florentina-Loredana Dragomir[1]

Abstract: A system information technology in security, intended saddle detector and saddle correct cognitive biases, are based on intelligence artificial intelligence (AI) and algorithms advanced to analyze data from multiple sources, such as government databases, IoT, and network social. This system combats cognitive biases, such as confirmation bias, anchoring effect, and delusion of truth, through learning techniques, checking information from multiple sources, and simulation AI algorithms to analyze dates to identify faults and provide decision-making alternatives. Also, the system promotes objectivity by anonymizing sources and comparing dates through cross-checking. systems information modern, which include mechanism advanced detection and correcting cognitive biases, are essential for improving process decision-making in security nation and international integration some analysis mechanisms behavior and verification of sources help prevent the spread of misinformation and erroneous interpretations, ensuring protection efficiency against risk emerging, including attacks terrorist. Thus, the technologies of advanced data processing and correcting cognitive biases will play a crucial role in the evolution of security systems, becoming a component indispensable in an increasingly world interconnected and complex, where threats of terrorists remain a concern overall major. To combat biases, the system integrates natural language processing (NLP) techniques and analysis behavioral, reducing influences subjective on decisions. The use of some source verification mechanisms and some comparative analyses helps prevent the spread of misinformation and reduce interpretation errors.

Keywords: cognitive biases; system information; cognitive models; security decisions

[1] Associate PhD, Faculty of Security and Defence, National Defence University Carol I, Bucharest, Romania, Address: 68-72 Panduri St., sector 5, 050662, Bucharest, Romania, Corresponding author: florentinaloredana.dragomir@gmail.com.

1. Introduction

In the world of systems information performance, man remains both the creator, how much and user of these technologies, influencing and being influenced by them. From the point of view psychologically, he is an essential factor in the process of decision-making (Dragomir, 2016a), having the ability to interpret shades of contextual information that algorithms can miss (Sallam, 2024). However, humans are vulnerable to their own cognitive biases, which can distort analysis and reactions to information provided by systems automated (Zou & Li, 2021a). Interaction man with these sistema redefines the concepts of trust, autonomy, and responsibility. On the one hand, algorithms can amplify decisions effectively and I can correct some limitations of humans (Zou & Li, 2024), but on the other hand part, I can introduce new risks, such as addiction excessive automation, or erosion capacity thus, man no longer is not just a decision maker, but an active participant in an ecosystem where we must saddle balance intuition, logical reasoning, and analysis data (Zou & Li, 2021b). In the future, as needed when AI becomes sophisticated, the role of humans could be reconfigured (Dragomir, 2016b). Instead of being the main decision-making factor, it It to become a systems supervisor, having a responsibility to interpret and validate decision algorithms (Dragomir, 2024). In addition, the system information incorporates elements of psychology humanity to become more adaptive, anticipating the needs of users and personalizing interaction (MacLean & Pincus, 2020). This man-machine symbiosis elevates challenges and ethical and philosophical issues related to control, responsibility, and equity decisions in an increasing world dominated by data and predictive models, strategies in cybernetics are directions key for predictive models of making security decisions (Sadeghiau & Khosravi, 2024).

2. System High-Performance Information Security with Detection and Correction of Cognitive Biases

A system information technology in the field of safety must be capable saddle collecting, analyzing, and objectively interpreting dates, reducing the impact of cognitive biases on decisions. This system It is saddle integrates models of advanced intelligence artificial intelligence (AI), bias detection algorithms, and decision adjustment mechanisms to ensure an assessment of how many precise threat

assessments and risks. System vulnerabilities are closely related to limitations in data, predictive models, and alert interpretation, and cognitive bias plays a significant role in amplifying these problems. Identifying and correcting bias is critical to increasing the effectiveness of these systems, thereby ensuring better risk anticipation and management. Effective early warning systems are essential for anticipating and managing economic, social, and security risks. These systems are often hampered by several vulnerabilities, including data quality, limitations of econometric models and AI algorithms, difficulties in interpreting alerts, cybersecurity risks, and reduced adaptability to economic changes. These vulnerabilities are often compounded by cognitive bias, which influences both the collection and analysis of data and the decisions based on it.

Figure 1. Vulnerabilities of the Cognitive Psychological Model

2.1. System Architecture and Components

2.1.1. Data Collection Component

The system receives information from multiple sources, such as government databases, intelligence sources, social networks, IoT sensors, and security reports. To reduce confirmation bias and the anchoring effect, the system applies source anonymization techniques and automatically verifies the information received through cross-checking methods.

2.1.2. Data Analysis and Processing Component

This compound used advanced artificial intelligence algorithms for data analysis and interpretation. The system uses:

- Neural networks for identifying complex patterns and detecting anomalies.
- Bayesian analysis for probability-based decision-making, providing multiple perspectives on a threat.
- Cognitive bias detectors, which identify systematic errors in data or decision-making. For example, if an analyst always makes decisions based on the same sources, the system flags this tendency and suggests alternative information.

2.1.3. Decision Simulation and Testing Mechanisms

The system includes a multi-scenario simulation module that generates decision alternatives and analyzes the impact of each option. This module is essential for combating hindsight bias (the tendency to see past events as more predictable than they were) and for assessing the impact of decisions before implementation.

2.1.4. User Interface and Feedback

A powerful system presents results in a format optimized for decision-making, using interactive visualizations, heatmaps, and alternative scenarios. To reduce the framing effect, the system offers users multiple ways to interpret the data, without biasing the analysis towards a single conclusion.

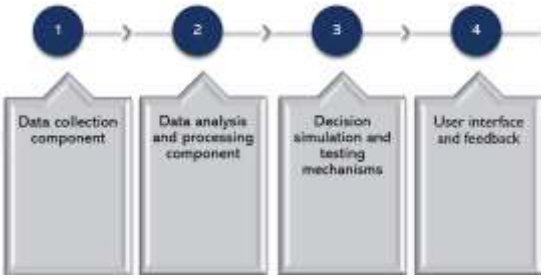

Figure 2. System information with Detection and Correction of Cognitive Biases

3. Detection and Correction of Cognitive Biases

In modern systems of information, detection and correction of cognitive biases are vital for making some decisions that are objectionable and informed. Cognitive biases influence interpretation dates and can lead to conclusions erroneous, affecting both factors human, how much and intelligence models artificial. In this context, it is crucial to integrate some mechanisms and advanced analysis tools that identify and correct such errors in systematic thinking.

Confirmation bias is one of the many common cognitive tendencies that affect the process of decision-making. This manifests itself by the selection and interpretation of information thus that saddle support beliefs pre-existing, excluding dates contradictory. The system information performances used technically advanced learning automatically to analyze the behavior of users and identify this trend. To counteract confirmation bias and intelligence algorithms I propose users' alternative perspectives, offering comparative analyses based on sources multiple. In addition, the systems impose checking information from sources different, reducing the risk of forming visions unilaterally on a subject. The anchoring effect influences making decisions by emphasizing excessive premium information received. This trend may determine users saddle isi based assessments on a reference point initially, without considering new data. To combat this effect, systems advance automatically generates scenarios counterfactuals, encouraging users to saddle analyze alternatives and saddle assess many possibilities. Intelligence algorithms present the user with a range variety of scenarios, using predictive models to highlight risks and opportunities, facilitating thus a process decision objective. Illusion truth is a phenomenon through which the information repeated is perceived as correct, regardless of its veracity. This error cognition is exploited frequently in disinformation campaigns and propaganda. To prevent this bias, the system information integrates source verification modules, which compare dates analyzed with information verified from trusted sources. In addition, disinformation detection algorithms point to users' content that poses a risk of high handling, while providing time fact-based comparative analysis objectives. This method provides a perception that may be clear on reality and reduces the impact of false information about process decision-making. Attribution bias affects the evaluation behavior of other entities, determining interpretation wrong based on prejudice and stereotypes. In the analysis of threats, this bias can lead to conclusions wrong, influencing security strategies and relations international. To eliminate these errors, systems information used technically advanced analysis behavior objectives. AI algorithms compare dates

available, calculate probabilities based on factors multiples, and offer interpretative alternatives, avoiding thus judgments based on prejudice growing or ideological. This approach allows making some decisions more accurate and reduces the risk of reactions disproportionate to the threat charges.

The integration of some mechanisms of effective detection and correcting cognitive biases is vital for the development of some Sistema information performances and fairness. By using artificial intelligence artificially and technologies advanced analysis, these systems can contribute significantly to improving process decision-making, eliminating influences subjective, and providing users a perspective balance and objective information analysis.

In the era of digitalization, social networks have become a resource important for the analysis of behavior and identification of potential threats. Posts public, discussion groups, and trends conversational allow detection of activity suspected or recruitment attempts for organizations extremists. However, to prevent interpretations wrong and to avoid spreading some false information, the system applies technically advanced verification, analyzing source, context, and validity of information by cross-checking methods. Another essential element of the data collection process is IoT (Internet of Things) sensors, which provide real-time information about various activities. These devices, used in infrastructure criticism, supervision trafficking, or monitoring perimeters sensitive, generate large volumes of data that require processing quickly and efficiently. The system uses intelligence algorithms artificial to analyze patterns identified and to detect behavior abnormal which would indicate a threat imminent. A key aspect of the data collection process is the reduction of confirmation bias, which can influence decisions by better information confirming assumptions initials. To combat this phenomenon, the system implements methods of anonymizing sources, thus that analysis to be achieved objectively, without influences caused by prejudices related to the origin information. Also, verification automatically through cross-checking allows the comparison of data from multiple sources independently, reducing thus the risk of making decisions based on incomplete information or erroneous. To increase the accuracy of the process, the system used natural language processing (NLP) techniques and learning automatic, so that saddle can quickly identify patterns suspicious in large volumes of unstructured data. Intelligence algorithms allow the extraction of information relevant from the text, comparing them with previous data sets and their classification based on A confidence score. This approach helps prioritize investigations and at the allocation resources efficiently. The data

collection component represents the foundation of any system high-performance information security system. Integration some various sources, application of some technically advanced verification, and the use of intelligence algorithms artificial are elements vital for the reduction of cognitive biases and growth efficiency in analysis threats. As appropriate as technology advances, this compound will become more and more sophisticated, allowing for the detection may quick and may accurate risk assessment, contributing thus to security nation and internationally. Paternal psychological analysis threats terrorist in analysis threats terrorist at the level internationally, various systems are used information advance to detect, monitor, and avert such dangers. An example notable is the "RED-Alert" project (Red Alert Detection System) early and real-time alert for content terrorists online), funded by the European Union European Union. This design proposes saddle development technology capable of saddle detector online radicalization and saddle support efforts for global counter-terrorism. RED-Alert uses processing natural language analysis networks social, intelligence artificial and processing complex of events to identify the content terrorist in real time. The project is coordinated by the Romanian company SIVECO. Another example is The System National Alert Terrorist (SNAT) of Romania, established in April 2004 at the proposal of Director Services Romanian Intelligence and approved by the Council Supreme Council of National Defense. SNAT has the role of establishing actions required for prevention or fight preparatory actions or carrying out some acts of terrorism on the territory of Romania. In 2019, the system was updated to ensure added clarity, flexibility, and pragmatism in establishing measures required by authorities. Also, at the level internationally, intelligence agencies collaborate to counteract new threats against safety globally.

These initiatives and satellite information demonstrate ongoing global efforts to use technology and cooperation international to prevent and combat threats terrorist. In the analysis of threats terrorist, systems information performance is based on a series of models psychological that help to understand and anticipate behavior human. Among the many uses, models have counted theory processing information, theory behavior planned, heuristic-systematic model, theory learning sociable, and theory framework interpretative. Theory processing information explains the way in which individuals collect, filter, and interpret information. In the context of the detection of threats of terrorists, this theory is used to analyze patterns of radicalization and to identify the ways in which extremist propaganda influences the perception and decisions of users. Theory behavior planning is used to understand the motivations

and intentions of actors involved in actions terrorist. This model allows evaluation of the probability that an individual saddle move from extremist discourse to action violent, based on factor cognitive and contextual factors that influence the decision. The heuristic-systematic model helps to identify cognitive biases that can affect both intelligence analysts, as well as and systems automated detection. This explains how people make decisions either through processes quick and intuitive (heuristics), or through analysis detailed (processing systematic). Systems information advanced are designed saddle balance these two types of processing to reduce the risk decisions based on biases cognitive. Theory learning sociable is essential in the analysis of radicalization and recruitment processes in groups of terrorist attacks. This model explains the way in which individuals adopt behavior by observation and interplay social. Intelligence systems artificially use this theory to detect networks of influence and to analyze how terrorist propaganda spreads online. Theory framework is interpretative (framing theory) analyzes the way the information is presented and how this work influences the collectible public. Systems to combat disinformation and radicalization use this theory to identify manipulative content and to create counter-narratives efficiently. By integrating these models' psychological systems information, threat analysis platforms terrorists are may effective in detecting and prevention attacks, while reducing time the impact of cognitive biases on process decision-making.

4. Conclusions

Developing a system of high-performance information for security, which integrates intelligence artificial and technically advanced detection and correcting cognitive biases is an essential step towards an assessment objective and precise threat reduction, influence factor subjective, such as confirmation bias and anchoring effects, allows making some decisions policy better substantiated, contributing to the protection of safety nation and international. Through the integration of some analysis mechanisms behavior and verification of sources, these systems help prevent the spread of misinformation and interpretations erroneous, ensuring protection efficiency against risk emerging technologies. Thus, advanced data processing and correcting cognitive biases will play a crucial role in the evolution of security systems, becoming a component indispensable in an increasingly world interconnected and complex. Reduction influence factor subjective, such as confirmation bias and anchoring effects, allows making some decisions policy better

substantiated, contributing to the protection of safety nationally and internationally. In the context of threats to terrorists, these systems are particularly valuable, providing the gear required for the identification and prevention of online radicalization and activities of extremists. Integration of some analysis mechanisms behavior and verification of sources helps prevent the spread of misinformation and erroneous interpretations, ensuring protection efficiency against risk emerging, including attacks terrorist. Thus, the technologies of advanced data processing and correcting cognitive biases will play a crucial role in the evolution of security systems, becoming a component indispensable in an increasingly world interconnected and complex, where threats terrorist remain a concern overall major. Initiatives such as the RED-Alert project and the National Alert Terrorist (SNAT) from Romania represent examples of important aspects of the use of technology advanced in the prevention and fight against terrorism. RED-Alert, with the help of intelligence artificially and processing language naturally, facilitates the detection of quick content online terrorists, in time what SNAT contributes to a response coordinated and effective in front of risk terrorist attacks. In the future, these Sistema will evolve continuously, integrating technology and algorithms to answer challenge emergent and to anticipate threats with increasing precision bigger.

References

Dragomir, F. L. (2016a). Models of Trust and Reputation in eCommerce. *OEconomica*, 12(6), 235-242.

Dragomir, F. L. (2016b). Recommendation and reputation in eCommerce. *EuroEconomica*, 25(2), 151-155.

Dragomir, F. L., Dumitriu, C., & Bărbulescu, A. (2021). Recommendation Systems-Modeling Abusive Clauses in E-commerce. *International Conference on Electrical, Computers, Communications and Mechatronics Engineering*, IEEE, 1-4.

MacLean, R. R. & Pincus, A. L. (2020). Cognitive Bias Modification for Addictive Disorders: Emerging Opportunities in Technology and the Treatment of Substance Use Disorders. *Psychiatry International*, 1(2), 75-82.

Sadeghian, A. & Khosravi, A. (2024). A Comprehensive Review of AI Techniques for Addressing Algorithmic Bias in Job Hiring. *AI*, 5(1), 383-404.

Sallam, M. (2024). The Era of Artificial Intelligence Deception: Unraveling the Challenges of AI Hallucinations, Misinformation, and Unpredictability. *Information*, 15(6), 299.

Zhou, Y. & Li, X. (2021a). A Survey on Bias in Deep NLP. *Applied Sciences*, 11(7).

Zhou, Y. & Li, X. (2021b). Cognitive Biases in Building Energy Decisions. *Sustainability*, 13(17).

Zhou, Y. & Li, X. (2024). A Comprehensive Approach to Bias Mitigation for Sentiment Analysis of Customer Feedback. *Applied Sciences*, 14(23).