RESEARCH ARTICLE

Analysis and Response Strategy of Cross-Community Rumors Using Mixed Multilayer Method for Enterprise Cyber Warriors

YI-WEI MA, CHUN-YAO CHANG, (Student Member, IEEE), YEN-NENG CHIANG, JIANN-LIANG CHEN, (Senior Member, IEEE), CHIH-HUNG CHEN, WEN-TSUNG CHANG, SHUN-CHING YANG, AND YING-HSUN LAI, (Member, IEEE)

1Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei 10607, Taiwan
2Department of Computer Science and Information Engineering, National Taiwan Normal University, Taipei 11677, Taiwan
3Cybersecurity Technology Institute, Institute for Information Industry, Taipei 106214, Taiwan
4Department of Computer Science and Information Engineering, National Taitung University, Taitung 95092, Taiwan

Corresponding author: Ying-Hsun Lai (yhlai@nttu.edu.tw)

ABSTRACT In the age of information explosion, it is easy for people to receive many messages, and it is difficult to verify the authenticity of each message. Therefore, people often quickly and forward the acquired information and share anonymous information, rather than absorbing it after verification. The study questions current Artificial Intelligence (AI) detection methods, arguing that a simple dichotomy cannot distinguish between true and false information. This study proposes a mixed method to analyze events based on the dissemination and interaction of false information in online enterprise communities from the perspective of an observer. The event explores multiple features based on various characteristics, such as motivation, purpose, intention, and behavior. Experimental results show that the proposed method can effectively identify false information with high risk. Additionally, this study discusses the effectiveness and response strategies of the enterprise cyber warrior based on the mixed multi-layer analysis. This study provides a preliminary study of mixed cognitive warfare identification and immediate response behavior for corporate Internet rumors.

INDEX TERMS Cross-community rumors, enterprise cyber warrior, enterprise information management, mixed analysis method, response strategies.

I. INTRODUCTION
Suppose an individual intends to influence the information cognition of relevant audience groups. They increase the popularity of an article by sharing or interacting with each other in the information dissemination process, realizing cognitive warfare. Without timely identification, analysis, or intervention, misinformation can spread rapidly on the Internet and may affect human cognition and behavior [1], [2], [3]. Some enterprises use the dissemination of information to influence trends in related issues and gain considerable attention to motivate a specific matter. For example, disinformation and deceptive articles spread everywhere during the 2016 US presidential election [4], [5], [6]. In the commercial, misinformation often misleads the public, affects consumption when products promote and causes goodwill impact. Therefore, enterprises must immediately analyze, identify, and build response strategies for the spread of cross-community Internet rumors before the damage expands. The abnormal correlation among communicators, broadcasters, and responders is challenging to analyze, and users can appear on different platforms in varying roles. A person may play multiple positions and exhibit malicious behavior in the form of groups [7]. Therefore, detecting abnormal interactions between various characters is time-consuming, requires a large amount of data for comparison or verification, and it is challenging to
observe real abnormalities [8]. In addition, when enterprises perceive cross-community rumors, they often do not know how to clarify them and even adopt wrong response strategies to increase the volume of rumors.

This study investigates practical challenges by identifying the information system used for enterprise Internet rumors and then organizing and analyzing them with a mixed multilayer method. An event system proposed can visualize an event’s attributes, including its properties, such as the article publishing time, publishing platform, article sentiment, and event associations. It can help users understand the development of events and observe the associations between events on different media. Enterprises can judge whether to respond to misinformation based on multi-layered rumor propagation analysis. The contributions of this study are as follows:

1) A mixed multi-layer method is proposed based on the difficulties in analyzing, identifying, and detecting misinformation systems for cyber warriors. This study includes the account, content, and communication points of the characteristics analysis and hazard quantification of behavioral characteristics. This study can assist users in identifying risky articles and events and appropriately disposing of them before the hazard expands.

2) A behavioral trait score table (BTST) and quantitative formula were proposed based on the collected case analysis results. The BTST can transform the characteristic behaviors of influential factors and hazards into a numerical representation. The quantitative formula can weigh the influence and risk of the event to obtain a weighted score, and then the user can compare the degree of hazard of the events using the weighted scores.

3) Enterprise response strategies were discussed with different cross-community communication models. This study provides a mixed multi-layer visualization to think about when and where to quickly clarify based on the different rumors and spread multi-layer patterns.

II. LITERATURE REVIEW

Zhang and Ghorbani [9] proposes and discusses detection methods, datasets, and future research directions. A clear guide for artificial news research is provided, but it can only provide past methodological reviews and expected future trends, and follow-up practice is still needed. Zhao et al. [10] explored the modeling of fake and factual news in dissemination. However, this study only analyzed the point-to-point transmission pattern and did not include the two-way forwarding and other transmission methods, which have limitations. Barbado et al. [11] proposed a framework for detecting false reviews and built an authenticity detection dataset for online reviews; the results provided an F-score of 82% for the classification task. However, essential differences between false reviews and false information remain, which cannot be directly transferred to authenticity detection in false information.

Xue et al. [12] outperformed existing methods at that time based on higher accuracy. However, the primary key factor of the network is the inherent characteristics of fake news, and it is challenging to extract intrinsic features. Based on natural language processing, Kumari et al. [13] proposed a deep multitask learning framework. Soprano et al. [14] proposed a multidimensional concept and used a crowdsourced method to generate fake news detection datasets with high reliability. The authors pointed out that the multidimensional approach is more reliable than the single-dimensional method. Although the author positively evaluated crowdsourcing behavior, there may still be malicious factors in building the dataset, which affects the quality.

Li et al. [15] proposed a method based on social cognitive theory. Allcott and Gentzkow [16] examined the impact of fake news and social media. Cao et al. [17] proposed detects abnormal users. Ozbay and Alatas [18] proposes a solution for the fake news detection.

Ozbay and Alatas [19] combine text analysis methods with supervised artificial intelligence algorithms to propose a model for detecting fake news. The model first uses text analysis techniques to extract structured data from unstructured news articles and then feeds the data into a supervised artificial intelligence algorithm.

Guo et al. [20] believe that emotion is an essential indicator for verifying the authenticity of social media information. Fake news usually requires strong emotions to attract readers’ resonance to achieve the purpose of spreading fake news. An Emotion-based Fake News (EFN) detection framework is proposed, which uses the content and comments of articles to learn semantic and emotional information, and uses three levels of Gate to use dynamic information fully. However, this method is mainly used in microblogs with limitations and pertinence compared with other methods. If it applies to other social software, its effect might reduce.

Gupta et al. [21] conducts a comprehensive survey of fake news, discusses its characteristics, origins, and conceptual models in detail, and visualize the motivations, dissemination mechanisms, and influence mechanisms of fake news. The study also analyzes solutions in the existing literature, categorizes solutions into four main types, and illustrates and analyzes them. The study also proposes an ideal solution, including three perfect solutions that need to be satisfied: Privacy-Preserving, ConText-Aware, and Fairness. However, it describes the obstacles posed by reality and the difficulties encountered in future research.

Parikh and Atrey [22] discuss five methods for detecting fake news. The future research direction proposed and the key integration is carried out, but this paper lacks experimental data and comparison results.

Seddari et al. [23] combine linguistic features, fact-verification features, and three types of information, including the publisher’s reputation, the number of publications, and the opinion of fact-checking sites about the publisher. The proposed method achieves higher accuracy using fewer features than other methods. Experimental results show that
using both features simultaneously can reach 94.4% accuracy, which is higher than the accuracy of using language features (89.4%) and fact-verification features (81.2%) separately. However, the fact-checking feature may not apply to other social media, as it may not necessarily have fact-checking capabilities.

Most of the existing methods are based on artificial intelligence algorithms, and the rest are primarily textual analyses of articles or analyses of communication types. However, the former has limited results because the fake information may be videos or pictures, and the latter cannot collect information comprehensively because of social media’s closed and anonymous nature. Therefore, there are still difficult challenges in researching fake news detection, and various attempts, analyses, and research are needed.

III. MOTIVATION
With the birth of artificial intelligence, big data and deep learning, today’s fake news detection methods are gradually changing to artificial intelligence and other methods for learning and detection to judge the right or wrong of news information. However, this study considers that information must not be simply distinguished from right or wrong, accurate or inaccurate, and true or false. After all, the message cannot be only pure right or wrong, because the information to be conveyed is likely to have different meanings or interpretations according to the change of a sentence from a word, or the affirmation or negation of a sentence, and thus lead to partial true or partially false information occurs, so it is impossible to directly judge whether the article is 100% true or 100% false. In this regard, this study proposes a new message analysis framework for the above issues. By analyzing the information such as the disseminator/account number, dissemination platform, and the positive and negative direction of the content, we can identify the trend of opinion conveyed by the message, the meaning behind it, and the goal that the conveyer wants to convey to identify the real purpose of this article, and through its purpose to find out what is the trend of public opinion that the article wants to bring? This study hopes that through this framework, it can be combined with the current artificial intelligence and other fake news discrimination methods to achieve more accurate fake news detection.

IV. RESEARCH OBJECTIVES AND MIXED METHODS
The overall research model divides the community rumors from two main perspectives: human and information technology, and collaboratively explore reaction strategies shown in Fig. 1. Furthermore, difficult and complex logical thinking procedures and related settings of system configuration, such as specific keywords, narrow time ranges, designated platforms for data search, various scoring, quantification-related regulations, and guidelines, are assigned to human processing. Information technology handles the processing of large amounts of computing; real-time monitoring; collection and processing of data; and related data analysis, such as crawlers, sentiment analysis, IP analysis of accounts, and horizontal and vertical interaction analyses of communication patterns.

A. DATA COLLECTION
Enterprise cyber warriors mainly use personal or news media to disseminate information in the online community, influence public opinion on a particular issue, and guide the public in a specific direction, achieving certain motives. Observed events found that certain types of news are desirable for people to click and watch. The types that were sorted and counted through observations are as follows.

1) REAL PICTURES AND FAKE TEXT
Netizens or reporters use their real photos and add fake text to create exciting meme pictures to attract people to watch and pass false news.

2) SATIRICAL ARTICLES OR JOKES
Ironic articles and jokes mock or ridicule other people’s remarks and articles to achieve entertainment effects to attract public attention and promote the news.

3) NEGATIVE EVENTS
Events related to violence or taint attract the public’s attention.

The research collects text data from powerful media platforms on the Internet based on the crawler module running in real time. This study collected information on events based on who, what, when, where, and which. “Who” includes the communicator, broadcaster, and responder. “What” includes specific keywords and events. “When” has posting time, modification time, deletion time, and posting frequency. “Where” has the platform website and IP location. “Which” includes positive and negative sentiment of the article, the number of links, and replies. After verifying the message, we can find its motivation, deduce why the person is bringing the news, and determine the message’s primary purpose. The search scope is limited and narrowed by the event keywords,
search scope, or the specific period provided by the user. This avoids crawling excessive uninteresting and redundant data, thus improving the search and analysis performance, and reducing the time cost.

**B. DATA ANALYSIS**

The study provides a mix method to analyze abnormal features that are difficult to detect intuitively. It constantly generates new information and news on the Internet, and presents quantitative results and visual data to users for understanding. The analysis had three main aspects: account, content, and communication.

Account analysis includes IP, abnormal behavior, and account history analyses.

1) **IP ANALYSIS**
   Using the user’s IP, check whether other users use the duplicate IP multiple times. Alternatively, verify whether users are connected utilizing a VPN or an overseas IP.

2) **ABNORMAL BEHAVIOR ANALYSIS**
   Detects the user’s current usage status and confirms whether there is an account that has been idle for a long time and has suddenly published influential articles. Evaluate whether the behavior pattern must be classified as abnormal or alerted [24].

3) **ACCOUNT HISTORY ANALYSIS**
   Collect behavior data, such as the user’s past posting, replying, and forwarding records, and analyze the user’s idioms, behavior patterns, stances, and tendencies, as a reference for whether the account may be abnormal. The content analysis includes text tagging, sentiment analysis, or similarity analysis.

4) **SENTIMENT ANALYSIS**
   Judging the sentiment tendency of the article content and dividing the sentiment of the text into positive, neutral, and negative, which can be used as a reference for the analysis of communication patterns [25].

5) **SIMILARITY ANALYSIS**
   This includes verifying the similarity in writing style and article content. Writing-style analysis detects whether the same author has written different articles. An article-content-similarity analysis detects the degree of similarity among various articles. If the similarity is significantly high, the sources of articles may be the same [26].

6) **TEXT TAGGING ANALYSIS**
   This record various pieces of information about each article, such as the number of replies or reposts, used as a reference for subsequent event graph drawing and the judgment of abnormal situations [27].

   The propagation pattern analysis included horizontal interaction, vertical interaction, and sound volume analyses.

7) **HORIZONTAL INTERACTION ANALYSIS**
   This focuses on interactive behaviors on the same platform, such as retweeting or commenting, and detects whether there is abnormal interaction between different accounts on the same platform. For example, cyber warriors always respond to or forward messages on specific account articles to increase attention.

8) **VERTICAL INTERACTION ANALYSIS**
   This focuses on interactive behavior across multiple platforms, and detects multiplatform interactive behavior—whether there is abnormal interaction between different accounts. For instance, they are especially reposting articles from news websites with a biased stance, only reposing articles published by certain journalists, or routinely sharing articles from politically minded flanking fans to increase exposure and discussion of other similar behaviors.

9) **SOUND VOLUME ANALYSIS**
   This focuses on the number of articles and discussions on each platform. In the sound-volume analysis of a single event, the sound volume of each forum should be positively correlated. Unless there are circumstances, usually, no single platform shows a sharp rise [28].

**C. MULTI-LAYER PROPAGATION PATTERN**

This study presents a schematic diagram of the events between different platforms, spaces, and times. This provides an understanding of how events on various platforms spread links, or the earliest occurrence and end time of events. This allows the observer to understand the entire event more intuitively and facilitates further observation of the event.

For the convenience of observation, this study gave different platforms fixed colors. In addition, other patterns were provided for different states of the event. According to the event plan, a three-dimensional structure is drawn to watch events unfold across different platforms, as shown in Fig. 2. The visual is drawn, which provides the user with final decision-making. This multi-layer propagation includes behavioral feature analysis, risk quantification, and visualization of the results.

**D. RISK ANALYSIS AND RESPONSE STRATEGIES**

This study organizes and summarizes the suggested behavioral-feature scoring methods based on account numbers, article content, dissemination patterns, and related event information. According to each social platform or news media’s information, their behavioral characteristics can be established. According to the collected case and behavioral trait score table, this study formulates a quantitative formula that provides a useful reference for identifying cyber warriors. Quantitative equitation uses the article as the main factor for scoring and performs quantized weighting of behavioral traits based on the article’s account, content, and communication.
The quantitative equation is shown in

\[ S = P_w \times \left( \sum_{a=0}^{2} A_{wa} \times \left( I_{wa} \times \left( \sum_{x=0}^{n_{a,1}} i_{wa,x} \times i_{sa,x} \right) \right) \right) + D_{wa} \times \left( \sum_{y=0}^{n_{a,2}} d_{wa,y} \times d_{sa,y} \right) \]  

Here, \( S \) is the total weighted score of risk, \( P_w \) is the weighted value of the platform, \( A_{wa} \) is the weighted value of the attribute, \( n_{a,1} \) is the number of influential characteristics for the specific attribute, \( n_{a,2} \) is the number of risk characteristics for the specific attribute, \( I_{wa} \) is the overall weighted value of all influential characteristics for the specific attribute, and \( D_{wa} \) is the overall weighted value of all risk characteristics for a specific attribute. \( P_w \) can be determined by evaluating the key observation area of the event; the default is 1. The sum of the overall weighted values of all influential and risk characteristics for a specific attribute was 1. Enterprises will be able to assist in judging response strategies based on risk analysis coefficients and cross-platform communication paths. If the risk factor is not high, it means that the enterprise rumor may not cause rapid spread, and the enterprise can use a cold treatment mechanism to avoid the echo effect. However, if the risk score is too high and occurs in a multi-platform interactive echo situation, the company should quickly clarify or cooperate with high-volume personnel to fight rumors to avoid anxiety for customers or reduce commercial purchase intentions.

V. CASE STUDY AND DISCUSSION

This study takes the case of an Asian company’s products being rumored as an example. When using mixed multi-layer analysis, we can quickly understand the overall rumor propagation speed and cross-platform orientation. Fig. 3 (a) shows the results according to the original post number with a decimal point plus a number to classify the replying articles. The system uses an arrow to point to the linked article if the reply has an attached link, as shown in Fig. 3 (b). When a user deletes an article during delivery, the event is recorded as a hollow circle, as shown in Fig. 3 (c).

In behavioral feature analysis, some programs contain subjective judgments; therefore, manual adjustment, configuration, and determination are required. The human part must establish, detect, and evaluate the account characteristics, content, and communication type. Behavioral factors can be divided into risk and influencing characteristics. Risk characteristics must be created based on the user’s position, inclination, and related information, such as a political stance against the user or a relatively insecure account IP location. The influence feature is the size of the possible influence of the account, article, communication type, or evaluation of the length of the expected communication chain. An account’s public persona, exposure rate, and other information can be listed as influencing characteristics.

The analysis results are quantified according to the listed behavioral characteristics. Different platforms, aspects...
(accounts, content, and dissemination types), and features (influence and risk characteristics) have many factors that affect each other. Therefore, it is recommended to assign individual weights when quantifying such that the final risk quantification score can be closer to the reality of the event. Event-related visualization diagrams are drawn based on various outcomes, such as event structure diagrams, quantification of risk levels, and event analysis results, after annotating warning signs to provide users with the final judgment of abnormal conditions. Through visual discovery, in this case rumors, rapid spread across platforms occurred during the incident. And if this can be clarified through the fast-spreading social platform, there is a better chance to eliminate the spread of rumors.

Fig. 4. is the system architecture proposed for this study. The process is as follows: first, obtain data from social media and news platforms, filter the text data by elements such as keywords, time and scope defined in advance, and then perform data pre-processing to reduce redundant text parts. Then, obtain the filter data and perform three types of analysis on it: account, content, and communication type. Finally, the analysis results are scored using the behavioral trait score table. Through the proposed quantitative formula, the converted scoring result into a quantitative risk value, which can use as a reference for the risk level of an article. Enterprises can deal with articles according to the risk level. The experimental method used in this study is manual data collection, pre-processing, and analysis, and the behavioral feature scoring table and initial weight are both self-defined. A review of many articles is required to define a behavioral trait score table effectively.

Table. 1. is the experimental results. The article numbered EN005 confirmed false information. The article account’s historical behavior and account information are very suspicious, and the article’s content is very controversial and emotional, so it gets a high score in BTST. EP003 is the main role of the article numbered EN005 cross-platform forwarding. Its content is also controversial and emotional, so it gets a higher...
VI. CONCLUSION
News and information spread rapidly and widely on the Internet through social media. This study proposed a mixed enterprise information system and architecture involving disseminators, time, and social platforms based on active observation to improve the ease of verifying enterprise Internet rumors. This work used a crawler module to collect data, analyze articles containing keywords scattered on the community platform, and extract their characteristics. For future research on misinformation or fake news, it is speculated that we could disseminate misinformation to provide good information by observing the behavior patterns of each user in the articles or responses. The event-structure diagram analyzes events from three aspects: account, content, and dissemination type, and provides the specific occurrence time, dissemination time of the event through the time axis of the event, and quiet time to facilitate the observation of the trend of the overall event. Event detection analyzes three aspects: the user account, article content, and propagation mode. It provides the specific occurrence, dissemination, and quiet times of the event to facilitate users to observe the overall event trend. Furthermore, analyzing the sentiment of the event articles and their comments, which includes positive, negative, and neutral sentiments, reflects whether the article is inconsistent with the other user opinions and is suspicious of a cyber warrior. This study also proposed a detailed behavioral-feature scoring table for the risk analysis and quantification of events to detect whether an event is risky. The case study showed that the mixed method can effectively detect the risk of an event in real time. Enterprises can also judge relevant response strategies through multi-layer graph visual methods to prevent harm caused by corporate rumors.

REFERENCES
[1] Y. Zhang, Y. Su, L. Weigang, and H. Liu, “Rumor and authoritative information propagation model considering super spreading in complex social networks,” Phys. A, Stat. Mech. Appl., vol. 506, pp. 395–411, Jan. 2018.
[2] A. Alamsyah and A. Sonia, “Information cascade mechanism and measurement of Indonesian fake news,” in Proc. 9th Int. Conf. Inf. Commun. Technol. (ICoICT), Aug. 2021, pp. 566–570.
[3] M. Alobaid and R. Ramachandran, “A social media case study on the impact of misinformation on business and consumers,” in Proc. 9th Int. Conf. Softw. Eng. Res. Innov. (CONISOFT), Oct. 2021, pp. 197–206.
[4] R. N. Zaem, C. Li, and K. S. Barber, “On sentiment of online fake news,” in Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM), Dec. 2020, pp. 760–767.
[5] C. Budak, “What happened? The spread of fake news publisher content during the 2016 U.S. Presidential election,” in Proc. World Wide Web Conf., 2019, pp. 139–150.
[6] A. Pal and A. Y. K. Chua, “Propagation pattern as a telltale sign of fake news on social media,” in Proc. 5th Int. Conf. Inf. Manage. (ICIM), Mar. 2019, pp. 269–273.
[7] I. Vogel and M. Meghana, “Detecting fake news spreaders on Twitter from a multilingual perspective,” in Proc. IEEE 7th Int. Conf. Data Sci. Adv. Anal. (DSAAn), Oct. 2020, pp. 599–606.
YI-WEI MA received the Ph.D. degree from the Department of Engineering Science, National Cheng Kung University, Tainan, Taiwan. He is currently an Assistant Professor with the National Taiwan University of Science and Technology. His research interests include the Internet of Things, cloud computing, future network, and ubiquitous computing.

CHUN-YAO CHANG (Student Member, IEEE) received the bachelor’s degree in software engineering and management from the National Kaohsiung Normal University, Taiwan. He is currently pursuing the degree with the National Taiwan University of Science and Technology. His research interests include the Internet of Things, software engineering development, and network technology research and development.

YEN-NENG CHIANG received the bachelor’s degree in electrical engineering from Chung Yuan Christian University, Taiwan. He is currently pursuing the degree with the National Taiwan University of Science and Technology. His research interests include the Internet of Things, software engineering development, and network technology research and development.

JIANN-LIANG CHEN (Senior Member, IEEE) was born in Taiwan, in December 1963. He received the Ph.D. degree in electrical engineering from the National Taiwan University, Taipei, Taiwan, in 1989. Since August 2008, he has been with the Department of Electrical Engineering, National Taiwan University of Science and Technology, where he is currently a Professor. His current research interests include directed at cellular mobility management and personal communication systems.

CHIH-HUNG CHEN received the Ph.D. degree in computer science and information engineering from the National Taiwan Normal University, Taipei, Taiwan, in 2021. He is currently a Postdoctoral Researcher with the Department of Computer Science and Information Engineering, National Taiwan Normal University. His research interests include computer games and artificial intelligence.

WEN-TSUNG CHANG received the B.S., M.S., and Ph.D. degrees in computer science from the National Chiao Tung University, Taiwan, in 1989, 1991, and 1995, respectively. He is currently acting as the Technology Director with the Cybersecurity Technology Institute (CSTI), Institute for Information Industry (III), Taiwan. His research interests include object-oriented design and programming, performance evaluation, distributed systems, and media processing on wireless and embedded systems. His major current research interests include artificial intelligence, FinTech/credit scoring, RPA (robotic process automation), big data analytics, smart tourism, IoT cybersecurity analytics, media forensics, and leads the teams to develop core data analysis technologies and services on the related application domains.

SHUN-CHING YANG received the B.S. degree in computer science from the National Chiao Tung University, in 2004, and the M.S. degree in electrical engineering from the National Taiwan University, in 2008. He is currently acting as the Section Manager with the Cybersecurity Technology Institute (CSTI), Institute for Information Industry (III). His major current research interests include influence operation, open source intelligence, and fake accounts detection on social media.

YING-HSUN LAI (Member, IEEE) received the Ph.D. degree from the National Cheng Kung University, Tainan, Taiwan, in 2013. He serves an Associate Professor at the Department of Computer Science and Information Engineering, National Taitung University. His research interests include STEAM education, AIoTs applications, and multicultural education.

VOLUME 10, 2022