INTERNATIONAL JOURNAL OF CYBER THREAT INTELLIGENCE AND SECURE NETWORKING (IJCTISN)

eISSN: 3087-4297

Volume. 02, Issue. 06, pp. 01-07, June 2025

EVOLVING PARADIGMS AND FUTURE TRAJECTORIES IN CYBER THREAT INTELLIGENCE

Dr. Layla Hassan
Department of Information Security, King Saud University, Riyadh, Saudi Arabia

Reem Al-Mazrouei
Emirates Center for Cybersecurity Research, United Arab Emirates University, Al Ain, UAE

Article received: 26/04/2025, Article Accepted: 15/05/2025, Article Published: 10/06/2025
DOI: https://doi.org/10.55640/ijctisn-v02i06-01

ABSTRACT

Cyber Threat Intelligence (CTI) has emerged as a cornerstone of modern cybersecurity, enabling organizations to anticipate, detect, and respond to evolving threats. As the cyber threat landscape becomes increasingly dynamic and complex, CTI paradigms are undergoing significant transformation. This paper explores the evolving paradigms of CTI, tracing its shift from reactive models to predictive and proactive frameworks driven by automation, artificial intelligence, and threat contextualization. Through a comprehensive analysis of current methodologies, tools, and applications, the study identifies key trends such as collaborative intelligence sharing, integration with Security Operations Centers (SOCs), and real-time threat hunting. It also examines the challenges in data quality, standardization, and adversarial deception. Finally, the paper outlines future trajectories for CTI, emphasizing the need for adaptive, interoperable, and intelligence-driven security ecosystems.

Keywords: Cyber Threat Intelligence (CTI), Evolving Cybersecurity Paradigms, Threat Detection, Predictive Intelligence, Intelligence Sharing, Threat Hunting, Security Automation, Cyber Defense, Adversarial Threats, Future Cybersecurity Trends.

INTRODUCTION

The contemporary digital landscape is characterized by an incessant and escalating barrage of cyber threats, ranging from sophisticated ransomware attacks that cripple organizations globally [2] to persistent advanced persistent threats (APTs) targeting critical infrastructure. In this volatile environment, traditional, reactive cybersecurity measures—focused primarily on perimeter defense and post-incident response—are proving increasingly insufficient. A proactive and predictive approach has become not just beneficial but imperative for safeguarding digital assets and ensuring operational continuity. This necessity has propelled Cyber Threat Intelligence (CTI) to the forefront of modern cybersecurity strategies.

Cyber Threat Intelligence refers to analyzed, refined, and contextualized information about current or potential threats and vulnerabilities that can be used to mitigate risks [31]. It moves beyond raw data (such as IP addresses or file hashes) to provide actionable insights into threat actors, their motivations, capabilities, tactics, techniques, and procedures (TTPs) [35, 36]. The primary goal of CTI is to enable organizations to make informed, data-driven decisions to enhance their defensive posture, anticipate attacks, and respond more effectively to security incidents [6, 33].

Despite its acknowledged importance, the field of CTI faces inherent complexities. The sheer volume, velocity, and variety of raw threat data available from disparate sources, including open-source intelligence, commercial feeds, and the dark web, present significant challenges for collection, processing, and analysis [5, 13, 16]. Furthermore, integrating CTI into existing security operations, ensuring its quality, and fostering effective information sharing across organizations remain persistent hurdles [9, 10, 21, 22, 23].

This article provides a comprehensive review of current approaches in Cyber Threat Intelligence, detailing the sources, mining techniques, and sharing mechanisms that underpin modern CTI practices. Furthermore, it delves into the significant challenges currently facing the CTI domain and proposes critical future directions, aiming to outline a roadmap for enhancing the effectiveness, actionability, and collaborative potential of CTI in the evolving cybersecurity landscape.

METHODS

This systematic literature review was conducted to synthesize and analyze the current state of Cyber Threat Intelligence (CTI) approaches and identify future directions, drawing exclusively from the provided set of 41 references. The methodology involved a structured process of information extraction, thematic categorization, and critical synthesis to ensure a comprehensive and evidence-based discussion.

1. Data Collection and Scoping: The foundation of this review was the complete list of 41 references provided by the user. These references spanned various formats, including academic papers, conference proceedings, technical reports, and online articles from reputable cybersecurity organizations and research institutions. No additional external sources were consulted beyond this defined set.

2. Information Extraction and Annotation: Each reference was systematically reviewed to extract key information pertinent to CTI. A detailed annotation process was followed, where specific data points, definitions, methodologies, challenges, and proposed solutions were identified and recorded. Special attention was paid to:

Core Concepts: Definitions of CTI, its benefits, and fundamental principles [2, 3, 4, 31, 35, 36].

Sources of CTI: Identification and characteristics of various data sources used for CTI, such as open-source intelligence, commercial feeds, dark web intelligence, and internal organizational data [5, 16, 18, 37, 38].

CTI Lifecycle/Phases: Descriptions of the typical stages involved in generating CTI, including collection, processing, analysis, and dissemination [5, 6].

Current Techniques/Approaches: Specific technical and methodological approaches employed in CTI mining, such as machine learning [7, 32], natural language processing, threat hunting [1, 24], and the use of standards [8, 25, 34, 40].

CTI Sharing Mechanisms: Discussions on the importance, benefits, challenges, and solutions related to sharing threat intelligence between entities [3, 4, 9, 10, 17, 18, 22, 26, 27, 28, 29, 30, 41].

Challenges and Limitations: Identified issues in CTI implementation and utilization, including data quality, volume, context, integration, legal aspects, and resource constraints [9, 10, 13, 17, 21, 22, 23].

Future Directions/Research Gaps: Suggestions for future research, emerging technologies, and strategic advancements in the CTI domain [1, 7, 11, 19, 20, 32, 39].

3. Thematic Synthesis and Categorization: Following the extensive data extraction, a thematic analysis approach was applied. The extracted information was grouped into logical categories, which directly informed the structure of the "Results" section. This categorization ensured a coherent presentation of current CTI practices and emerging trends. Key thematic areas included:

Sources of CTI

The CTI Lifecycle and Methodologies

The Role of Machine Learning and Automation

CTI Standards and Formats

CTI Sharing Landscape

Actionability of CTI

4. Discussion and Future Outlook: The synthesized findings from the "Results" section formed the basis for the "Discussion." This part involved a critical evaluation of the current state, addressing the identified challenges, and proposing concrete future directions, drawing linkages between the different thematic areas. The aim was to provide a forward-looking perspective on how CTI can evolve to meet the escalating demands of cybersecurity.

This rigorous methodological approach ensured that the review was comprehensive, well-structured, and firmly grounded in the provided references, enabling a thorough exploration of current CTI approaches and their future trajectories.

RESULTS

The comprehensive review of the provided literature reveals a dynamic and evolving landscape of Cyber Threat Intelligence (CTI), characterized by diverse sources, increasingly sophisticated mining techniques, and a growing emphasis on collaborative sharing. The findings detail the foundational components and current practices that define the state-of-the-art in CTI.

I. Sources and Lifecycle of Cyber Threat Intelligence

Effective CTI generation begins with the robust collection of raw data from various sources, which then undergoes a structured lifecycle to transform into actionable intelligence.

Diverse CTI Sources: Threat intelligence originates from a multitude of sources, each offering unique insights [16]. These include:

Open-Source Intelligence (OSINT): Publicly available information such as security blogs, news feeds, industry reports, social media, and academic research. This provides broad context and early warnings of emerging threats [18].

Commercial Threat Intelligence Feeds: Subscription-based services from cybersecurity vendors that provide curated, validated, and often machine-readable indicators of compromise (IoCs), malware analyses, and adversary profiles [16]. Crowdstrike [35] and Kaspersky [36] are examples of companies providing such services.

Dark Web Intelligence: Information gleaned from clandestine forums, marketplaces, and communication channels on the dark web, offering insights into threat actor methodologies, planned attacks, and stolen data [37].

Technical Intelligence: Derived from deep analysis of malware samples, network traffic, intrusion attempts, and forensic data. This yields specific IoCs like malicious IP addresses, domain names, and file hashes [38].

Internal Organizational Data: Logs from security devices (firewalls, IDS/IPS), SIEM systems, vulnerability scans, and incident response reports provide invaluable context specific to an organization's own environment.

The CTI Lifecycle: Regardless of the source, raw threat data typically progresses through a structured lifecycle to become actionable intelligence [5, 6]. This lifecycle includes:

Collection: Gathering raw data from various sources.

Processing: Cleaning, normalizing, and enriching the raw data.

Analysis: Applying analytical techniques to uncover patterns, identify relationships, and derive insights (e.g., threat actor TTPs, motivations).

Dissemination: Delivering the finished intelligence to relevant stakeholders in an understandable and timely manner, often through threat intelligence platforms.

II. Current Approaches and Methodologies in CTI Mining

The transformation of raw data into actionable intelligence relies heavily on advanced analytical techniques and automation.

Automation in CTI: Automated systems are critical for handling the immense volume and velocity of threat data. This involves automated collection, parsing, and initial correlation of IoCs and other threat data [5]. The drive towards automated threat-informed cyberspace defense is a key area of development [19].

Machine Learning (ML) and Artificial Intelligence (AI): ML and AI play a pivotal role in extracting actionable insights from large, complex, and often unstructured CTI data [7, 32].

Threat Detection: ML algorithms are used for anomaly detection in network traffic and system logs, identifying suspicious patterns that might indicate an attack [7].

Malware Analysis: AI assists in the automated analysis and classification of malware variants.

Natural Language Processing (NLP): NLP is crucial for parsing and understanding human-readable threat intelligence from security blogs, forums, and reports, enabling the extraction of entities, relationships, and attack narratives [32].

Predictive Analytics: ML can be used to forecast future attack trends or identify potential targets based on historical data.

Threat Hunting: CTI fuels proactive threat hunting activities, where security analysts actively search for undetected threats within their networks using intelligence on adversary TTPs and IoCs [1]. This includes automated threat hunting in specialized environments like industrial control systems (ICS) [24].

Standardization of CTI Formats: To facilitate interoperability and sharing, various standards and frameworks have been developed. STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information) are prominent examples for structuring and exchanging CTI [8, 25, 34, 40]. These standards are crucial for building automated and integrated CTI solutions.

III. Cyber Threat Intelligence Sharing

The collaborative sharing of CTI is recognized as a cornerstone of collective cyber defense, enhancing the security posture of individual organizations and the broader ecosystem.

Benefits of Sharing: Sharing CTI leads to several advantages, including improved situational awareness, faster detection and response times, reduced costs, and the ability to leverage a collective defense against common adversaries [10, 26, 27, 28, 29]. It helps in

understanding the broader threat landscape beyond an organization's immediate perimeter.

Challenges in Sharing: Despite the benefits, significant barriers impede effective CTI sharing:

Trust and Confidentiality: Organizations are often reluctant to share sensitive information due to concerns about trust, potential exposure of their vulnerabilities, or competitive disadvantages [9, 22].

Legal and Regulatory Issues: Data privacy regulations (e.g., GDPR) and liability concerns can complicate or restrict the sharing of certain types of threat information [17, 22].

Technical and Format Incompatibilities: Inconsistent data formats, differing taxonomies, and a lack of standardized APIs make it difficult to integrate CTI from various sources [13, 14, 16, 22].

Lack of Actionability and Context: Shared intelligence may lack sufficient context, making it difficult for recipients to determine its relevance or how to act upon it [10].

Solutions and Models for Sharing: Efforts are underway to address these challenges:

Decentralized Incentives: Research explores decentralized incentive mechanisms to encourage threat intelligence reporting and exchange, potentially using blockchain technologies to enhance trust and traceability [9, 30].

Information Sharing and Analysis Organizations (ISAOs): These sector-specific or community-based platforms facilitate trusted information sharing among members [15, 26].

Situational Awareness Platforms: Solutions designed to improve cybersecurity situational awareness and information sharing, particularly for public administrations, often leverage advanced big data analysis [18].

Shared Solutions for SMEs: Tailored solutions are emerging to help small and medium-sized enterprises (SMEs) overcome resource limitations and participate in CTI sharing [41].

DISCUSSION

The preceding review underscores that Cyber Threat Intelligence has matured into an indispensable component of modern cybersecurity, moving beyond merely reactive defense to enable proactive and predictive security strategies. However, while current approaches have made significant strides, particularly in automated collection and the application of machine learning, several critical challenges persist, necessitating a clear vision for future directions.

Persistent Challenges in Current CTI Approaches

Despite technological advancements, the effective operationalization of CTI faces significant hurdles:

Data Overload and Signal-to-Noise Ratio: The sheer volume of raw threat data from various sources can lead to information overload for security analysts, making it difficult to discern critical signals from irrelevant noise [13]. This often results in "analysis paralysis" and delayed response. The quality of CTI feeds also varies, with concerns about false positives and the currency of information [21].

Lack of Context and Actionability: A common critique is that much of the available CTI lacks the necessary context to be directly actionable for an organization's unique environment. Raw IoCs without accompanying TTPs, actor profiles, or impact assessments offer limited value [10, 33]. The process of converting generic intelligence into insights specific to an organization's assets and vulnerabilities remains a significant challenge [23].

Integration and Interoperability: Despite the existence of standards like STIX/TAXII [25, 34, 40], seamless integration of CTI into existing security information and event management (SIEM), security orchestration, automation, and response (SOAR), and other security tools remains complex. This often leads to fragmented security operations and inhibits automated response capabilities.

Trust and Collaboration Barriers: While the benefits of CTI sharing are well-established [27, 29], overcoming the inherent trust deficit between organizations, compounded by legal ambiguities and competitive concerns, continues to be a major obstacle [17, 22]. This limits the collective defense potential against global threats.

Resource Constraints: Many organizations, especially smaller ones [41], lack the specialized human talent and financial resources required to establish and maintain a mature CTI program, including dedicated analysts, sophisticated tools, and robust intelligence platforms.

Future Directions in Cyber Threat Intelligence

To address these challenges and maximize the potential of CTI, several critical future directions emerge:

Hyper-Automated and AI-Driven CTI: The future of CTI lies in the continued development and widespread adoption of highly automated, AI-driven systems capable of real-time collection, processing, and analysis of threat

data. This includes advanced machine learning for predictive analytics (forecasting attack trends), deep learning for sophisticated malware analysis and anomaly detection, and natural language generation for contextualizing and summarizing complex threat narratives automatically [7, 19, 32]. Such automation will alleviate analyst fatigue and accelerate response times.

Contextualization and Personalization: Future CTI platforms must prioritize the delivery of highly contextualized and personalized intelligence. This involves systems that can automatically map generic threat intelligence to an organization's specific assets, vulnerabilities, and business risks. This shift from "information overload" to "relevant insights" will make CTI truly actionable.

Decentralized and Trust-Enhanced Sharing Ecosystems: Overcoming sharing barriers requires innovative approaches. Blockchain-based solutions for secure, transparent, and auditable CTI sharing show promise by enhancing trust and accountability in distributed environments [30]. Furthermore, the development of federated learning approaches could allow collaborative threat model building without direct sharing of raw, sensitive organizational data. Efforts like CS-AWARE project for local public administrations are steps in this direction [18].

Focus on Emerging Threat Vectors: As the attack surface expands, CTI must evolve to address new and emerging threat vectors. This includes:

Internet of Things (IoT) and Industrial Internet of Things (IIoT) Security Intelligence: Given the proliferation of interconnected devices, CTI needs to specifically focus on vulnerabilities, threats, and attack patterns targeting IoT and IIoT devices and cyber-physical systems [14, 20, 39].

Supply Chain Intelligence: With increasing sophistication of supply chain attacks, CTI must provide deeper insights into the security posture of third-party vendors and the entire digital supply chain.

Offensive Cyber Counterintelligence: Exploring offensive cyber counterintelligence techniques to understand adversary capabilities and intentions more deeply, as suggested by Sigholm and Bang [11], can provide invaluable insights for proactive defense.

Human-AI Collaboration (Augmented Intelligence): While automation will increase, human analysts will remain crucial for strategic insights, nuanced interpretation, and decision-making. Future CTI systems should focus on augmenting human intelligence, enabling analysts to ask complex questions, validate AI-generated insights, and contribute their unique expertise.

In conclusion, Cyber Threat Intelligence is at a pivotal juncture. The transition from a data-heavy, often reactive discipline to a highly automated, context-aware, and proactively integrated function is paramount. By embracing advanced AI/ML, fostering trusted collaborative ecosystems, and focusing on emerging threat landscapes, CTI can truly empower organizations to move beyond mere defense to achieve anticipatory and resilient cybersecurity postures in an increasingly complex digital world.

REFERENCES

1. Aldauiji, F., Batarfi, O., & Bayousif, M. (2022). Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art. IEEE Access.

2. Statista. (2024). Statista-report. Retrieved March 14, 2024, from https://www.statista.com/topics/4136/ransomware/#topicOverview

3. Lutf, M. (2018). Threat intelligence sharing: a survey. Journal of Applied Science and Computation, 8(11), 1811–1815.

4. Zrahia, A. (2018). Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views. Journal of Cybersecurity, 4(1), tyy008.

5. Borges Amaro, L. J., Percilio Azevedo, B. W., Lopes de Mendonca, F. L., Giozza, W. F., Albuquerque, R. D., & García Villalba, L. J. (2022). Methodological framework to collect, process, analyze and visualize cyber threat intelligence data. Applied Sciences, 12(3), 1205.

6. Gandotra, V., Singhal, A., & Bedi, P. (2012). Threat-oriented security framework: A proactive approach in threat management. Procedia Technology, 4, 487–494.

7. Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. Journal of Defense Modeling and Simulation, 19(1), 57–106.

8. de Melo e Silva, A., Costa Gondim, J. J., de Oliveira Albuquerque, R., & García Villalba, L. J. (2020). A methodology to evaluate standards and platforms within cyber threat intelligence. Future Internet, 12(6), 108.

9. Menges, F., Putz, B., & Pernul, G. (2021). DEALER: Decentralized incentives for threat intelligence reporting and exchange. International Journal of Information Security,

20(5), 741–761.

10. Pala, A., & Zhuang, J. (2019). Information sharing in cybersecurity: A review. Decision Analysis, 16(3), 172–196.

11. Sigholm, J., & Bang, M. (2013). Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats. In 2013 European Intelligence and Security Informatics Conference (pp. 166–171). IEEE.

12. Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: The security incident response perspective. IEEE Communications Surveys & Tutorials, 23(4), 2525–2556.

13. Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10(1), 371–379.

14. Fortino, G., Savaglio, C., Spezzano, G., & Zhou, M. (2020). Internet of things as system of systems: A review of methodologies, frameworks, platforms, and tools. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51(1), 223–236.

15. Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. NIST Special Publication, 800(150).

16. Ramsdale, A., Shiaeles, S., & Kolokotronis, N. (2020). A comparative analysis of cyber-threat intelligence sources, formats and languages. Electronics, 9(5), 824.

17. Nweke, L. O., & Wolthusen, S. (2020). Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection. In 12th International Conference on Cyber Conflict (CyCon) (Vol. 1300, pp. 63–78). IEEE.

18. Schaberreiter, T., Roning, J., Quirchmayr, G., et al. (2019). A cybersecurity situational awareness and information-sharing solution for local public administrations based on advanced big data analysis: The CS-AWARE project. In Challenges in Cybersecurity and Privacy – The European Research Landscape (pp. 149–180).

19. Mavroeidis, V. (2021). Towards automated threat-informed cyberspace defense.

20. Pal, S., Hitchens, M., & Varadharajan, V. (2020). Access control for Internet of Things—Enabled assistive technologies: An architecture, challenges and requirements. In Assistive Technology for the Elderly (pp. 1–43). Elsevier.

21. Griffioen, H., Booij, T., & Doerr, C. (2020). Quality evaluation of cyber threat intelligence feeds. In International Conference on Applied Cryptography and Network Security (pp. 277–296). Springer.

22. Zibak, A., & Simpson, A. (2019). Cyber threat information sharing: Perceived benefits and barriers. In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1–9).

23. Oosthoek, K., & Doerr, C. (2021). Cyber threat intelligence: A product without a process? International Journal of Intelligence and CounterIntelligence, 34(2), 300–315.

24. Arafune, M., Rajalakshmi, S., Jaldon, L., et al. (2022). Design and development of automated threat hunting in industrial control systems. In IEEE International Conference on Pervasive Computing and Communications Workshops (pp. 618–623).

25. Czekster, R. M., Metere, R., & Morisset, C. (2022). CyberaCTIve: A STIX-based tool for cyber threat intelligence in complex models. arXiv preprint arXiv:2204.03676.

26. Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security, 60, 154–176.

27. Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, Article 101589.

28. Du, L., Fan, Y., Zhang, L., Wang, L., & Sun, T. (2020). A summary of the development of cyber security threat intelligence sharing. International Journal of Digital Crime and Forensics (IJDCF), 12(4), 54–67.

29. Sukhabogi, S., et al. (2021). A theoretical review on the importance of threat intelligence sharing & the challenges intricated. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(3), 3950–3956.

30. Xiaohui, Z., & Xianghua, M. (2021). A

reputation-based approach using consortium blockchain for cyber threat intelligence sharing. arXiv preprint arXiv:2107.06662.

31. McMillan, R. (2013). Definition: Threat intelligence. Gartner.com.

32. Montasari, R., Carroll, F., Macdonald, S., Jahankhani, H., Hosseinian-Far, A., & Daneshkhah, A. (2021). Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence. In Digital Forensic Investigation of Internet of Things (IoT) Devices (pp. 47–64). Springer.

33. Pawlinski, P., Jaroszewski, P., Kijewski, P., Siewierski, L., Jacewicz, P., Zielony, P., & Zuber, R. (2014). Actionable information for security incident response. European Union Agency for Network and Information Security, Heraklion, Greece.

34. Doerr, C. (2018). Cyber threat intelligence standards – a high-level overview. TU Delft CTI Labs.

35. CrowdStrike-CTI. (2022). Retrieved May 31, 2022, from https://crowdstrike.com/cybersecurity-101/threat-intelligence/

36. Kaspersky-CTI. (2022). Retrieved March 20, 2022, from https://kaspersky.com/resource-center/definitions/threat-intelligence/

37. Samtani, S., Li, W., Benjamin, V., & Chen, H. (2021). Informing cyber threat intelligence through dark web situational awareness: The AZSecure hacker assets portal. Digital Threats: Research and Practice (DTRAP), 2(4), 1–10.

38. Bou-Harb, E., Debbabi, M., & Assi, C. (2013). Cyber scanning: A comprehensive survey. IEEE Communications Surveys & Tutorials, 16(3), 1496–1519.

39. Pal, S., & Jadidi, Z. (2021). Analysis of security issues and countermeasures for the industrial Internet of Things. Applied Sciences, 11(20), 9393.

40. Farnham, G., & Leune, K. (2013). Tools and standards for cyber threat intelligence projects. SANS Institute.

41. van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Răcătăian, A., Baumgartner, L., Fricker, S., Ruiz, J. F., et al. (2021). A shared cyber threat intelligence solution for SMEs. Electronics, 10(23), 291.

42. Dip Bharatbhai Patel. (2025). Incorporating Augmented Reality into Data Visualization for Real-Time Analytics. Utilitas Mathematica, 122(1), 3216–3230. Retrieved from https://utilitasmathematica.com/index.php/Index/article/view/2690