ISR Journal of Economics, Business and Management (ISRJEBM)

Homepage: https://isrpublisher.com/isrjebm/

Volume 01, Issue 02, December 2025 ISSN: 3108-1517 (Online)

OPEN ACCESS

Craft Trade in Cybersecurity and Digital Forensics: Shaping The Future of Cyber Threat Intelligence, Counterintelligence and Espionage. Amid Global E-Crime Challenges

Yousef Elzidani[1]*, Dr. Syed Jafri[2]

[1]Student at the University of the West of England (UWE Bristol), Studying BSc (Hons) Cyber Security and Digital Forensics, Coldharbour Ln, Stoke Gifford, Bristol BS16 1QY, United Kingdom
[2]Senior Lecturer, Henley Business School, UOR, University of Reading, Whiteknights Rd, Reading RG6 6UD, United Kingdom

***Corresponding author:** Yousef Elzidani
Student at the University of the West of England (UWE Bristol), Studying BSc (Hons) Cyber Security and Digital Forensics, Coldharbour Ln, Stoke Gifford, Bristol BS16 1QY, United Kingdom

Article History

Received: 12-10-2025

Accepted: 12-11-2025

Published: 17-11-2025

Abstract: **Original Research**

The internet has become an integral part of society. In contrast, despite this increased significance, it is being employed as a tool for interfering in the domestic affairs of countries, compromising national security, and impairing economic structure. Therefore, in the current business and political landscape, cybersecurity is a major concern in all areas for firms as well as nations. As enterprises and countries are adapting to the technological revolution, protecting technological resources turns out to be quite critical. This domain is a main growth sector as the nature and magnitude of threats are evolving and increasing. The increased magnitude and intricacy of cyber assaults are impacting the performance of organisations globally. Therefore, the teams coordinate in order to overcome intricate cyberattacks. In this research paper, the systematic review-based methodology is employed in order to find the role of craft trade and cyber threat intelligence in the field of cybersecurity. The significance of craft trade in the context of cybersecurity is investigated. Moreover, the merits and demerits of cybersecurity craft trade are documented. The utilisation of CTI by the intelligence community to anticipate and prevent threats is explored. The ways to enhance the effectiveness of threat intelligence in order to anticipate, detect and give effective responses to cyber incidents are delved into.

Keywords: Cybersecurity, Cyber Threat, Network Security, Cyber Threat Intelligence, Threat Intelligence, Cyber Attack.

1. INTRODUCTION

In the current business and political landscape, cybersecurity is a major concern in all areas for firms as well as nations. As enterprises and countries are adapting technological revolution, protecting technological resources turn out to be growingly critical (Rawindaran, 2025). Nations and organisations employ cybersecurity to protect their data centres and technological infrastructure. An effective cybersecurity strategy safeguards a company's and a country's infrastructure and important information from cyber threats which can impact the digital infrastructure gravely (Štitilis, 2016). Firms and countries utilise it to avoid different sorts of threats, including information breaches, phishing, and ransomware, etc. This domain is a main growth sector as the nature and magnitude of threats are evolving and increasing (Ciuriak, 2024). Every country is enhancing its defence capabilities, including cyber capabilities (Goel, 2020).

1.1. Background

There is growth in innovation with the growth of the internet. The internet has become an integral part of society. In contrast, despite this increased significance, it is being employed as a tool for interfering in the domestic affairs of countries, compromising national security, and impairing economic structure. To overcome these cyber risks and employ during disputes, nations have started to develop their digital capabilities (Mishra, 2019). It incorporates misinformation-based campaigning, sabotaging threats, assessing cyber strategies and collecting intelligence. The nations will keep enhancing their digital capabilities as restraint against adversaries. The countries need to be vigilant regarding the significance of the internet and comprehend threats to society (Goel, 2020).

Different countries waged cybersecurity attacks against their rivals in order to destabilise them, undermine national security and fetch critical information. For instance, Operation Aurora started in 2006 by China. It was a malware assault on the major US organisations. It incorporated attacks on more than 140 firms across all domains between 2006 and 2014. Likewise, in 2010, a worm was made by the US and Israel in order to target the nuclear infrastructure of Iran through infiltrating infection in PLCs of the centrifuge machines of nuclear reactors, which made them dysfunctional (Goel, 2020).

2. Literature Review

2.1. Definitions

2.1.1. Craft Trade

Craft trade is the act of acquiring and communicating secret information. Digital craft trade strategies always employ the latest technological systems. The effective craft trade should have to be uncomplicated, safe, and secret (Miller, 2000).

2.1.2. Cyber Threat Intelligence

It is intricate cyber risk data which is gathered by assessing the current insights. It includes various malware categories employed in breaches or groups of risk actors incorporated. Such information is quite critical for comprehending and anticipating breaches and risk development (Brown, 2015).

2.2. Major Cybersecurity-related Challenges

The several major cybersecurity-related challenges which are evolved with the advancement in technology which are as:

2.2.1. The Ever-varying Threats

The ever-varying nature of possible threats is one of the major challenges. The latest cyber threats have evolved with the advancement in technology. Therefore, it is vital to enhance cyber capabilities for overcoming ever-changing cyber-attacks (Ballamudi, 2022).

2.2.2. Gigantic Volume of Data

Organisations normally possess a gigantic volume of information regarding their clientele and potential clients. Therefore, there is a greater probability of ransomware attacks to fetch this vulnerable critical information stored on cloud servers. The firms need to have a fool proof cyber strategy to protect digital resources (Bodepudi, 2021).

2.2.3. Workforce Training

The education of the workforce is quite significant in countering threats. They should be better equipped by means of training to avoid threats and take appropriate measures in case of any breach (Gutlapalli, 2019).

2.2.4. Scarcity of Skilled Workforce

Another serious challenge is the scarcity of skilled workforce at a time when humongous number of attacks are being carried out, impacting thousands of firms greatly. There is a high demand for skilled technical manpower who can mitigate the possibilities (Mandapuram, 2018).

2.3. Sorts of Cyber Security

2.3.1. Vital Infrastructure Cybersecurity

The reliance of SCADA systems on outdated software makes the systems vulnerable to cyber threats. As per NIS regulations, the firms providing basic services in the UK should have adequate cybersecurity in place.

2.3.2. Network Security

It is about tackling susceptibilities which impact the operating systems, network systems, incorporating servers, hosts, and firewalls, etc.

2.3.3. Cloud Security

It is about safeguarding confidential data saved in the cloud, incorporating applications, and information.

2.3.4. Internet of Things Security

It is about making the smart gadgets secure which are connected to the internet.

2.3.5. Application Security

It is about addressing susceptibilities which originate from insecure development processes related to programming and designing software and websites (Mandapuram, 2020).

2.4. Requirement for a Consolidated Cybersecurity Intelligence

Formerly, the organisations used to have standalone cybersecurity measures personalised as per possible threats. In the current business landscape, the teams coordinate in order to overcome intricate cyberattacks. It is because of the following factors:

2.4.1. Sophisticated Threats

Conventional cybersecurity strategy is not effective in detecting and overcoming the latest cyberthreats. Therefore, a detailed and comprehensive strategy is needed to overcome different modern threats, including advanced persistent threats.

2.4.2. Intricated Environments

The corporate network infrastructure is comprised on-premises as well as multiple cloud servers. Therefore, it is quite challenging to keep such intricate infrastructure secure (Thaduri, 2016).

2.4.3. Diverse Endpoints

Information technology is not just confined to computers. The companies' digital resources are saved on various types of devices. In some organisations, the workforce works from home by staying connected with organisational networks. Therefore, it is needed to protect all these devices, which is a challenging job.

Hence, organisations can handle these evolving threats effectively by a consolidated approach and streamlined network infrastructures (Fadziso, 2023). The increased magnitude and intricacy of cyber assaults are impacting the performance of organisations globally. Despite the fact that firms are increasingly investing in their cybersecurity to prevent cyber assaults, the elements impacting their cybersecurity deployment are scattered. Furthermore, the use of the latest technologies in cybersecurity has a high positive impact on the organisational performance (Hasani, 2023).

2.5. Examples of Cyber Craft Trade

WannaCry ransomware assault was carried out on the NHS in 2017. It impacted records of hospitals all over the country and demanded ransom in digital currency. Therefore, the NHS deployed threat intelligence which identified the threat and confined its scale massively. Similarly, the financial sector remained a main target of such cyber assaults. A renowned banking firm employed threat intelligence to identify and hamper the latest phishing attack. Pinpointed the involved group, analysed its strategies, identified and anticipated signs, and deployed measures.

Different developed countries assist developing countries in enhancing their cybersecurity capabilities, such as Australia. Likewise, the US and Japan collaborate with each other to improve their cybersecurity capabilities (Kang, 2022).

3. Methodology

3.1. Research Design

The current research paper's methodology is based on a systemic review of pertinent current literature for investigating the significance of craft trade in cybersecurity and digital forensics incorporating the way it is shaping the future of cyber threat intelligence, counterintelligence and espionage, merits of craft trade, and the way intelligence community employ the CTI to anticipate and prevent threats.

3.2. Search Strategies

The systematic review-driven methodology of this paper is based on Petticrew and Roberts (2006). The different key terms are used to search in various literature repositories. In order to enhance the extent of search in this paper, the references and in-text references are searched. In order to meet the objectives of this research journal, the main key term 'craft trade' regarding the cybersecurity of companies as well as countries was employed. The various literature repositories are searched, such as Research Gate, Scopus, Science Direct, Web of Science, and Grey Literature. The various other key terms are employed, including "craft trade", "cybersecurity craft trade", "network security", "cyber threat", "cyber threat detection", "cybersecurity threat intelligence", "consolidated threat intelligence" and "merits of cybersecurity craft trade". The titles, abstracts, as well as keywords of papers are searched with the help of terms to search and find relevant literature.

The focus remained on the publications which are relevant to craft trade in the cybersecurity domain. The above-mentioned key terms are employed in order to find the most relevant, latest and credible publications. These publications include research papers, conference proceedings, and reports, etc. Through inclusion criteria, abstracts of pertinent journals are analysed for adding peer-reviewed papers. These journals have to be pertinent to cybersecurity as well as cyber threat intelligence.

Various publications are not included as per the exclusion criteria. All the research papers which are not relevant to the cybersecurity domain are not included. Likewise, the publications which are relevant to cybersecurity but not to craft trade or threat intelligence are disregarded. Furthermore, the papers which are not focused on cybersecurity and threat intelligence are disregarded. The terms 'craft trade ' or 'cybersecurity', or 'threat intelligence' are mentioned in those digital resources 1-3 times. Initially, 56 publications are shortlisted. However, 16 of these were not added as they were not relevant to the variables, so the 40 are selected for the subsequent stage. Then references, including in-text references and references lists of the articles, are analysed. By employing regression, the shortlisted publications are 3. Additionally, through forward reference snowballing of 40 articles, 10 more are considered. In total, 53 papers are considered for systemic review. These publications are re-analysed for making sure the relevance and quality of content.

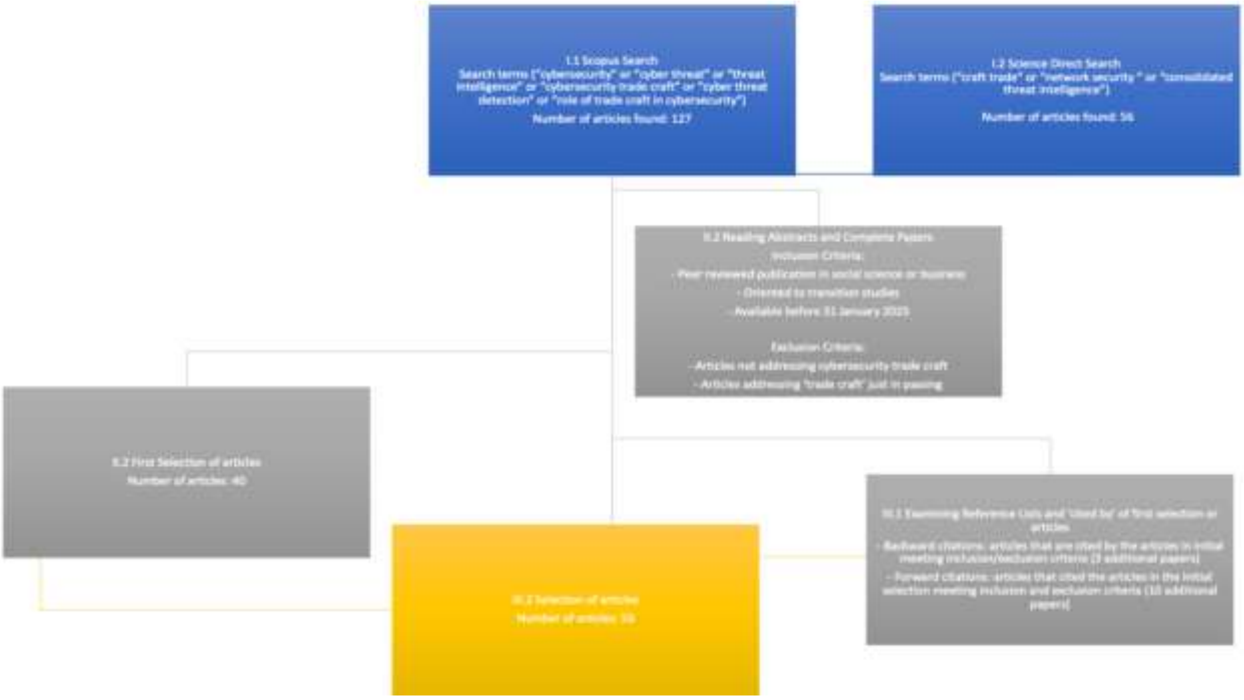
I.1 Scopus Search
Search terms ("cybersecurity" or "cyber threat" or "threat intelligence" or "cybersecurity trade craft" or "cyber threat detection" or "role of trade craft in cybersecurity")
Number of articles found: 127
I.2 Science Direct Search
Search terms ("craft trade" or "network security " or "consolidated threat intelligence")
Number of articles found: 56
II.2 Reading Abstracts and Complete Papers
Inclusion Criteria:
- Peer reviewed publication in social science or business
- Oriented to transition studies
- Available before 31 January 2025
Exclusion Criteria:
- Articles not addressing cybersecurity trade craft
- Articles addressing 'trade craft' just in passing
II.2 First Selection of articles
Number of articles: 40
III.1 Examining Reference Lists and 'Cited by' of first selection or articles
- Backward citations: articles that are cited by the articles in initial meeting inclusion/exclusion criteria (3 additional papers)
- Forward citations: articles that cited the articles in the initial selection meeting inclusion and exclusion criteria (10 additional papers)
III.2 Selection of articles
Number of articles: 53

Figure 1: Flow of systematic review

4. Findings

4.1. Significance of Craft Trade

There is a focus of governments and companies on securing digital assets by employing technology, however, the issue still persists. According to the information, the solution is not technology. The knowledge of cyber hackers gives them an edge. They have better information regarding the target than the target has about them. They can build the latest technological systems secretly and carry out assaults from an unknown location all over the world. Therefore, it is not possible for the network experts to gather, analyse and spread threat intelligence quickly or have relative information supremacy. Consequently, the cyber professionals need to comprehend the offensive cyber craft trade for forecasting and countering hackers (Wilcox, 2016).

The focal point of intelligence is to prevent, react and recover. Furthermore, these actions are operational and strategic and foster mutual trust between different stakeholders. The data dissemination is that a stakeholder had to disseminate data as per law to others. In contrast, intelligence sharing is the exchange of relevant insights while considering transparency and confidentiality. Coordination is the management of connections between dependent stakeholders, which requires the sharing of insights and technical expertise for aligning the objectives which these stakeholders are trying to achieve (Kianpour, 2020).

All over the globe, countries and firms have teams for collecting information regarding threats for remaining vigilant and safeguarding from assaults. They share data as they require external data in addition to gathered internal information for having a detailed outlook of the risk landscape. The data is gathered from a number of sources, such as commercial, open-source sources and digital communities. The readily available information is not a high-level indicating factor of breach, like available malware hash numbers or command-and-control IP addresses, so countermeasures can be implemented through a system in an automated manner. Efficient intelligence management systems are required to streamline production, improvement and assessment of information. However, the major constraint in this regard is acquiring information from various intelligence sources, integrating and enhancing information for better and relevant intelligence (Brown, 2015).

4.2. Employment of CTI by Intelligence Community to Anticipate and Prevent Threats

There is a surge in advanced cyber assaults, which is a serious challenge to conventional cybersecurity, such as polymorphic malware, as well as Advanced Persistent Threats. These threats are making conventional measures less effective in identifying and countering assaults (Milajerdi, 2019). Therefore, network experts have to formulate an effective strategy to overcome these assaults. The concentration should be on the capabilities of hackers instead of just on one's own susceptibilities (Caltagirone, 2013). The adversaries have the advantage of obscuring their identities and capabilities (Liao, 2016).

The vital data regarding hackers and an assault can be accessible with the progression of an assault. At this point, the Cyber Threat Intelligence is useful as it is a number of intelligence products for assisting the comprehension and prevention of current and possible future assaults (Qamar, 2017). These products are also termed as Indicators of Compromise. The low-level IOCs include exploration of filenames, hostnames, and IP addresses. The high-level IOCs include Tactics, Tools, and Procedures (Alsaheel, 2021). The CTI is successful if it is addressing the multiple requirements of the intelligence community, including appropriate information sharing as well as decreasing its overburden (Noor, 2019). It assists in reducing the possible inappropriate intelligence by sharing the appropriate data with appropriate persons at appropriate times (Marrin, 2004), or sinking in gigantic volumes of irrelevant data (Weinbaum, 2018).

CTI is improved by employing statistical and ML algorithms (Saeed, 2023; Salim, 2023; Souri, 2018). Natural Language Processing is employed in cyber attribution (Perry, 2019; Ren, 2023) and extricating Indicators of Compromise in an automated manner out of unstructured content in risk intelligence documents (Husari, 2017). Deep learning is utilised in cyber attribution (Rosenberg, 2017) as well as threat detection (Deliu, 2017). Statistical machine learning techniques, including anomaly detection and Random Forests, are effectively employed in this domain (Landauer, 2019; Xiao, 2024).

Experts are looking to apply LLMs in this field for learning patterns in information from various sources to predict, identify, attribute and categorise assaults with growingly high precision (Zhang, 2024; Marrin, 2017; Bang, 2016). However, the intelligence community has apprehensions regarding the quality of CTIs (Oosthoek, 2021). The CTI products are not transparent as proofs cannot be evaluated again, but the capacity to reassess proofs is a must for superior quality intelligence (Heuer, 1999). As per Oosthoek and Doerr (2021), data-empowered CTI does not allow validation of information sources and translations of proofs. According to experts, the reason is that IOCs are provided by commercial firms with no advantage to share their sources (Oosthoek, 2021).

The optimum way of handling this lack of transparency issue of IOCs and substandard CTI is to include techniques from conventional craft trade into CTI by employing human intelligence experts who can utilise CTI as an assistance in conventional hypothesis-based intelligence assessment. The AI-based computation is mandatory for greater amounts and speeds of inflowing information. The experts can employ the results of these computational tools as assistance (Mandiant, 2019). Moreover, Jadidi and Lu (2021) proposed a way in which experts are incorporated in assessing computationally built theories (Jadidi, 2021).

4.3. Merits and Demerits of Craft Trade in Cybersecurity

Cyber intelligence craft trade assists in enhancing the competencies of companies carrying out cyber intelligence. It is being carried out by means of explaining the optimum practices and mock running of solutions to common threats (Ludwick, 2013). Digital craft trade is employed to fetch the information regarding the different possibilities of threat, patterns of previous cyber incidents and details of cyber intruders. This cyber intelligence allows organisations and countries in anticipating and detecting the threats in a timely manner in order to avoid unfavourable consequences. Furthermore, the role of cyber intelligence craft trade is to recover appropriately in case of any cyber incident, in addition to preventing cyber incidents and giving a response to these cyber incidents (Miller, 2000).

The cyber intelligence craft trade shares the vital insights with countries to ensure their national security and allows to fosters strategic cooperation with allies (Cunliffe, 2023). By means of employing artificial intelligence in craft trades, the detailed data can be fetched in an automated manner, which allows for carrying out threat analysis, strategic analysis and reporting. The cyber experts have a pivotal role in analysing this information from different digital tools and drafting effective and appropriate cyber intelligence in time (Ettinger, 2019).

Rid stated that the nature of active measures is covert. Therefore, this secret nature makes the craft trade less effective (Rid, 2020). Countering the latest and ever-changing nature of cyber intrusions is the biggest challenge. The new ways of breaches are becoming available with the advancement in technology and cybersecurity measures (Ballamudi, 2022).

Nowadays, threat intelligence is an increasingly known phenomenon, in which firms or countries share insights, I-e indicators related to cyber risks, to a trusted community for risk assessment and attack response. Conversely, this exchange of insights increases numerous vulnerabilities to a firm which is concerned regarding its safety, confidentiality and competitiveness (Al-Ibrahim, 2017).

4.4. Enhancing Effectiveness of Threat Intelligence

The objective is not to exchange information; however, it is the way to accomplish the objective. It is also critical to explicitly state what sort of information is required to be exchanged, and what's the purpose of sharing information and how it is shared. In order to make this information exchange successful, it is critical for enterprises to recognise that what sort of insights are required from other organisations and what the expectations are from this information exchange with different corporations' actions (Yokohama, 2018). It is also vital for firms to pursue their own cybersecurity projects and efficiently employ their own insights before initiating information sharing. The objectives of collecting information include being aware of the latest risks, making decisions and implementing these vital decisions.

In order to make threat intelligence effective, every single component of information sharing is required to be improved. The shared information is categorised into multiple components, such as indicators, vulnerabilities, courses of action, incidents, threat actors, campaigns, TPP (tactics, techniques, and procedures), and analytical reports. Indicators must be comprised of data that allow quick identification, or what is relevant to the source of the assault. Susceptibilities are shortcomings spotted in particular software and data related to the threshold of risks which they exhibit. The course of action is an activity for risks and attacks. Particular IP addresses should be blocked effectively, application utilisation must be limited appropriately, and other relevant activities. Accurate and diverse data collection regarding attacks and adversaries who commit assaults (Nguyen, 2017).

The TTP must be included with effective information related to activities of hackers, particular assault strategies and technologies, and susceptibilities which cause assaults. Campaigns are required to be comprised of accurate data incorporating profiles of hackers, their objectives, and relevant attacks. Reports must be comprised of effective, quick and strategic decisions. Threat intelligence reports include existing assaults from security firms and public companies. Moreover, advisories and alerts and logs of efficacious and inefficacious initiatives and practices employed by members are also incorporated in shared information (Yokohama, 2018).

5. CONCLUSION

An effective cybersecurity strategy safeguards a company's and a country's infrastructure and important information from cyber threats which can impact the digital infrastructure gravely. Firms and countries utilise it to avoid different sorts of threats, including information breaches, phishing, and ransomware, etc. The different sorts of cybersecurity are vital infrastructure cybersecurity, network security, cloud security, internet of things (IOT) security and application security. The major cybersecurity-related challenges are the ever-varying threats, the gigantic volume of data, workforce training, and the scarcity of skilled workforce. The consolidated cybersecurity intelligence is required due to sophisticated threats, intricate environments, and diverse endpoints. The increased magnitude and intricacy of cyber assaults is impacting the performance of organisations globally. There is a surge in advanced cyber assaults, which is a serious challenge to conventional cybersecurity, such as polymorphic malware, as well as Advanced Persistent Threats. These threats are making conventional measures less effective in identifying and countering assaults. Despite the fact that firms are increasingly investing in their cybersecurity to prevent cyber assaults, the elements impacting their cybersecurity deployment are scattered.

The governments and companies have employed technology for securing their digital assets, but it is not quite effective in overcoming the latest and ever-evolving threats. The knowledge of cyber hackers gives them an edge as they build the latest technological systems secretly and carry out assaults from an unknown location all over the world. Therefore, it is not possible for the network experts to gather, analyse and spread threat intelligence quickly or have relative information supremacy. Therefore, the cyber professionals need to comprehend the offensive cyber craft trade for forecasting and countering hackers. Efficient intelligence management systems are required to streamline production, improvement and assessment of information. However, the major constraint in this regard is to acquire information from various intelligence sources, integrating and enhancing information for better and relevant intelligence. The CTI is successful if it is addressing the multiple requirements of the intelligence community, including appropriate information sharing as well as decreasing its overburden. It assists in reducing the possible inappropriate intelligence by sharing the appropriate data with appropriate persons at the appropriate time.

CTI is improved by employing statistical and ML algorithms. Natural Language Processing is employed in cyber attribution and extricating Indicators of Compromise from unstructured content in risk intelligence documents. Deep learning is utilised in cyber attribution (Rosenberg, 2017) as well as threat detection. Statistical machine learning techniques, including anomaly detection and Random Forests, are effectively employed. Experts are looking to employ LLMs for learning patterns in information from various sources to predict, identify, attribute and categorise assaults with growingly high precision. The optimum way of handling the lack of transparency issue of IOCs and substandard CTI is to include techniques from conventional craft trade into CTI by employing human intelligence experts who can utilise CTI as an assistance in conventional hypothesis-based intelligence assessment. Hence, the latest technologies with experienced network experts must be employed to counter the advanced and sophisticated cyber-attacks.

REFERENCES

- Al-Ibrahim, O. M. A. &. K. C., 2017. Beyond Free Riding: Quality of Indicators for Assessing Participation in Information Sharing for Threat Intelligence. *Cryptography and Security*. [Accessed 15 May 2025].
- Alsaheel, A. Y. N. &. M. S., 2021. . *ATLAS: A sequence-based learning approach for attack investigation.*. s.l., In Proceedings of the 30th USENIX Security Symposium., p. 3005–3022. [Accessed 15 May 2025].
- Štitilis, D. P. P. &. ,. I. M., 2016. Preconditions of sustainable ecosystem: cyber

security policy and strategies. *Journal of Entrepreneurship and Sustainability Issues,* 2(4), pp. 174-182. [Accessed 15 May 2025].

- Ballamudi, V. D. H. &. M. M., 2022. Influence of Digitization on Human Resources (HR) Services and Processes. *ABC Research* , 10(3), p. 32–36. [Accessed 15 May 2025].
- Bang, M., 2016. Pitfalls in military quantitative intelligence analysis: Incident reporting in a low intensity conflict. *Intelligence and National Security,* 31(1), p. 49–73. [Accessed 15 May 2025].
- Bodepudi, A. R. M. &. M. M., 2021. Algorithm Policy for the Authentication of Indirect Fingerprints Used in Cloud Computing. *American Journal of Trade and Policy,* 8(3), pp. 231-238. [Accessed 15 May 2025].
- Brown, S. G. J. &. S. O., 2015. *From Cyber Security Information Sharing to Threat Management.* s.l., s.n., pp. 43 - 49. [Accessed 15 May 2025].
- Brown, S. G. J. &. S. O., 2015. *From cyber security information sharing to threat management.* ,. New York, Association for Computing Machinery, p. 43–49. [Accessed 15 May 2025].
- Caltagirone, S. P. A. &. B. C., 2013. *The Diamond Model of Intrusion Analysis. Technical Report. Center For Cyber Intelligence Analysis and Threat Research Hanover Md.,* s.l.: Center For Cyber Intelligence Analysis and Threat Research Hanover Md. [Accessed 15 May 2025].
- Ciuriak, D., 2024. *Cybersecurity, National Security and Trade in the Digital Era* , s.l.: Ciuriak Consulting Inc. [Accessed 15 May 2025].
- Cunliffe, K., 2023. Cyber-enabled craft trade and contemporary espionage: assessing the implications of the craft trade paradox on agent recruitment in Russia and China. *Intelligence and National Security,* pp. 1-20. [Accessed 15 May 2025].
- Dasgupta, D. A. Z. &. S. S., 2022. Machine learning in cybersecurity: A comprehensive survey.. *J. Def. Model. Simul.* , Volume 19, p. 57–106. [Accessed 15 May 2025].
- Deliu, I. L. C. &. F. K., 2017. *Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks.* s.l., IEEE, p. 3648–3656. [Accessed 15 May 2025].
- Ertel, W., 2024. *Introduction to Artificial Intelligence.* Delhi: Springer Nature. [Accessed 15 May 2025].
- Ettinger, J., 2019. *Cyber Intelligence Craft trade Report* , Pittsburgh : Carnegie Mellon.
- Fadziso, T. T. ,. U. &. D. ,. S., 2023. Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat. 3(1). [Accessed 15 May 2025].
- FTC, 2015. *"Internet of Things: Privacy and Security in a Connected World".* [Online] Available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013- workshop-entitled-internet-things-privacy/150127iotrpt.pdf.workshop-entitled-internet-things-privacy/150127iotrpt.pdf [Accessed 15 May 2025].
- Goel, S., 2020. National Cyber Security Strategy and the Emergence of Strong Digital Borders. *Connections: The Quarterly Journal,* 19(1), pp. 73-86. [Accessed 15 May 2025].
- Gutlapalli, S. M. M. &. R. M., 2019. Evaluation of Hospital Information Systems (HIS) in terms of their Suitability for Tasks. *Malaysian Journal of Medical and Biological Research,* 6(2), pp. 143-150. [Accessed 15 May 2025].
- Hasani, T. O. N. &. D., 2023. Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics* , 3(97). [Accessed 15 May 2025].
- Heuer, R., 1999. Psychology of Intelligence Analysis. *Center for the Study of Intelligence.* [Accessed 15 May 2025].
- Husari, G. A.-S. E. &. A. M., 2017. *TTPDrill: Automatic and accurate extraction of threat actions from unstructured text of CTI sources..* s.l., ACM. [Accessed 15 May 2025].
- Jadidi, Z. &. L. Y., 2021. A threat hunting framework for industrial control systems. *IEEE* , p. 164118–164130. [Accessed 15 May 2025].
- Kang, J. H. M. &. A. R., 2022. *Unlocking the Potential of Digital Services Trade in Asia and the Pacific.* s.l.:ADB. [Accessed 15 May 2025].
- Kianpour, M., 2020. Knowledge and Skills Needed to Craft Successful Cybersecurity Strategies. *Norsk IKT-konferanse for forskning og utdanning.* [Accessed 15 May 2025].
- Landauer, M. S. F. &. W. M., 2019. *A framework for cyber threat intelligence*

extraction from raw log data. s.l., IEEE, p. 3200–3209. [Accessed 15 May 2025].

- Liao, X. Y. K. &. B. R., 2016. *Acing the IOC game: Toward automatic discovery and analysis of open-source cyber threat intelligence.*. s.l., In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, p. 755–766. [Accessed 15 May 2025].
- Ludwick, M. M. J. &. M. A., 2013. Cyber Intelligence Craft trade Project: Summary of Key Findings. [Accessed 15 May 2025].
- Maddireddy, B., 2024. Advancing Threat Detection: Utilizing Deep Learning Models for Enhanced Cybersecurity Protocols. *Rev. Esp. Doc. Cient.*, Volume 18, p. 325–355. [Accessed 15 May 2025].
- Mandapuram, M. &. H. M., 2018. The Object-Oriented Database Management System versus the Relational Database Management System: A Comparison. *Global Disclosure of Economics and Business,* 7(2), pp. 89-96. [Accessed 15 May 2025].
- Mandapuram, M. R. M. &. B. A., 2020. Application of Artificial Intelligence (AI) Technologies to Accelerate Market Segmentation. *Global Disclosure of Economics and Business,* 9(2), pp. 141-150. [Accessed 15 May 2025].
- Mandiant, L., 2019. *Going ATOMIC: Clustering and Associating Attacker Activity at Scale.* [Online] Available at: https://www.mandiant.com/resources/blog/clustering-and-associating-attacker-activity-at-scale [Accessed 15 May 2025].
- Marrin, S., 2004. Preventing intelligence failures by learning from the past. *International Journal of Intelligence and CounterIntelligence* , 7(4), p. 655–672. [Accessed 15 May 2025].
- Marrin, S., 2017. Understanding and improving intelligence analysis by learning from other disciplines. *Intelligence and National Security,* 32(5), p. 539–547. [Accessed 15 May 2025].
- Milajerdi, S. G. R. E. B. &. S. R., 2019. *Real-time apt detection through correlation of suspicious information flows. In Proceedings of the 2019 IEEE Symposium on Security and Privacy*. s.l., IEEE, p. 1137–1152. [Accessed 15 May 2025].
- Miller, R., 2000. Digital Craft trade: Espionage and Security in the Information Age. pp. 125-135. [Accessed 15 May 2025].
- Mishra, N., 2019. The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance. *Journal of World Trade.* [Accessed 15 May 2025].
- Nasir, V. &. S. F., 2021. A review on deep learning in machining and tool monitoring: Methods, opportunities, and challenges. *Int. J. Adv. Manuf. Technol.* , Volume 115, p. 2683–2709. [Accessed 15 May 2025].
- Nassar, A. &. K. M., 2021. Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. *J. Artif. Intell. Mach. Learn. Manag.*, Volume 5, p. 51–63. [Accessed 15 May 2025].
- Nguyen, K. R. H. &. J. R., 2017. Valuing information security from a phishing attack. *Journal of Cybersecurity,* 3(3), p. 159–171. [Accessed 15 May 2025].
- Noor, U. A. Z. &. M. A., 2019. A machine learning framework for investigating data breaches based on semantic analysis of adversary’s attack patterns in threat intelligence repositories. *Future Generation Computer Systems,* Volume 95, p. 467–487. [Accessed 15 May 2025].
- Oosthoek, K. &. D. C., 2021. Cyber threat intelligence: A product without a process?. *International Journal of Intelligence and CounterIntelligence,* 34(2), p. 300–315. [Accessed 15 May 2025].
- Perry, L. S. B. &. P. R., 2019. No-doubt: Attack attribution based on threat intelligence reports. In Proceedings of the 2019 IEEE International Conference on Intelligence and Security Informatics.. *IEEE,* p. 80–85. [Accessed 15 May 2025].
- Qamar, S. A. Z. &. R. M., 2017. Data-driven analytics for cyber-threat intelligence and information sharing. *Computers and Security,* Volume 67 , p. 35–58. [Accessed 15 May 2025].
- Rawindaran, N. J. A. &. P. E., 2025. Cybersecurity Framework: Addressing Resiliency in Welsh SMEs for Digital Transformation and Industry 5.0. *J. Cybersecur. Priv.*, 5(2), p. 17. [Accessed 15 May 2025].
- Razzaq, K. &. S. M., 2025. Machine Learning and Deep Learning Paradigms: From

Techniques to Practical Applications and Research Frontiers. *Computers,* 14(93). [Accessed 15 May 2025].

- Ren, Y. X. Y. &. Z. Y., 2023. Cskg4apt: A cybersecurity knowledge graph for advanced persistent threat organization attribution.. *IEEE Transactions on Knowledge and Data Engineering* , 35(6), p. 5695–5709. [Accessed 15 May 2025].
- Rid, T. &. F. S., 2020. Active Measures: The Secret History of Disinformation and Political Warfare. p. 513. [Accessed 15 May 2025].
- Riese, F. &. K. S., 2020. . Supervised, semi-supervised, and unsupervised learning for hyperspectral regression. Hyperspectral Image. *Anal. Adv. Mach. Learn. Signal Process.* , p. 187–232. [Accessed 15 May 2025].
- Rosenberg, I. S. G. &. D. E., 2017. *DeepAPT: Nation-state APT attribution using end-to-end deep neural networks.* s.l., Springer International Publishing, p. 91–99. [Accessed 15 May 2025].
- Saeed, S. S. S. &. A.-G. M., 2023. A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors 23*, Volume 16, p. 7273. [Accessed 15 May 2025].
- Salim, D. S. M. &. K. P., 2023. A systematic literature review for APT detection and effective cyber situational awareness (ECSA) conceptual model. *Heliyon* , 9(7). [Accessed 15 May 2025].
- Sarker, I., 2021. Deep cybersecurity: A comprehensive overview from neural network and deep learning perspective. *Sn Comput. Sci*, Volume 2, p. 154. [Accessed 15 May 2025].
- Souri, A. &. H. R., 2018. A state-of-the-art survey of malware detection approaches using data mining techniques.. *Human-centric Computing and Information Sciences*, 8(1), p. 1–22. [Accessed 15 May 2025].
- Thaduri, A. G. D. &. K. M., 2016. *Maintenance 4.0 in Railway Transportation Industry*. s.l., s.n., p. 317–331. [Accessed 15 May 2025].
- Tirulo, A. C. S. &. D. K., 2024. Machine learning and deep learning techniques for detecting and mitigating cyber threats in IoT-enabled smart grids: A comprehensive review. *Int. J. Inf. Comput. Secur.* , Volume 24, p. 284–321. [Accessed 15 May 2025].
- Verma, R., 2024. CYBERSECURITY CHALLENGES IN THE ERA OF DIGITAL TRANSFORMATION. p. 187. [Accessed 15 May 2025].
- Weinbaum, C. &. J. N., 2018. Intelligence in a data-driven age. *Joint Force Quarterly: JFQ* , p. 4–9. [Accessed 15 May 2025].
- Wilcox, M., 2016. *Countering Cyber Adversary Craft trade.* [Online] Available at: https://www.tripwire.com/state-of-security/countering-cyber-adversary-craft trade?utm_source=chatgpt.com [Accessed 15 May 2025].
- Xiao, N. L. B. &. W. T., 2024. APT-MMF: An advanced persistent threat actor attribution method based on multimodal and multilevel feature fusion. *Computers and Security* , p. 144. [Accessed 15 May 2025].
- Yokohama, S., 2018. *Business Management and Cybersecurity*, s.l.: NTT. [Accessed 15 May 2025].
- Zhang, J. B. H., &. W. H., 2024. When LLMs Meet Cybersecurity: A Systematic Literature Review. *A Systematic Literature Review.* [Accessed 15 May 2025].