Detection Tools for Cognitive Warfare: Leveraging the Cyber Domain

Robin Burda
Joštova 10
Brno, 602 00
CZECHIA

robin.burda@fss.muni.cz

ABSTRACT

Cognitive Warfare (CW) has emerged quickly in the past years and quite possibly presents one of the greatest threats to NATO countries. With the information overload in a complex world, making timely and informed decisions is hard, especially without the ability to detect adversarial CW operations quickly. The primary enabler for successful CW is cyberspace, which is already a complex domain with its own significant threats. However, it is also well understood, and many tools already exist to scan cyberspace for malicious content and adversarial operations. Without in-depth multidisciplinary analysis, much valuable time and experience will be lost, and the threat of CW cannot be adequately addressed. This paper aims to map the current state-of-the-art research and technology for monitoring cyberspace and assess the possibility of leveraging the existing knowledge for dealing with CW. The primary focus will be on indicators & warnings and assessment phases, as those are the first and necessary parts of a successful and timely defence against CW. The result of the research will be an overview of tools and methods with potential use for CW monitoring evaluated using pre-set criteria. This paper also constitutes a basis for SAS-185 Indicators and Warnings for Cognitive Warfare in Cyberspace.

Keywords: Cognitive warfare, Cyberspace, Detection tools, Indicators, Warnings

1.0 INTRODUCTION

While Cognitive Warfare (CW) is a concept that emerged only recently, the overlap with psychological warfare, hybrid threats, and propaganda allows researchers and practitioners to build upon solid existing knowledge. Claverie and Cluzel also specifically define CW as an "unconventional form of warfare that uses cyber tools" [1]. Cyberspace can be considered one of the key enablers for CW, and the fast-paced environment of the domain makes indicators and warnings complex and necessary. However, it also opens up possibilities to utilize the experience and existing tools devised for monitoring cyberspace [2]. Detection of CW activity in cyberspace should, therefore, work with such solutions as much as possible to free up resources for covering the defence gaps.

This paper aims to map existing tools for monitoring cyberspace and assess which can be used for similar purposes in regard to CW. This overview will also clarify the gaps in both knowledge and capabilities related to CW detection. To map out the landscape of cyber monitoring tools, I will review academic sources and relevant commercial solutions for monitoring CW in cyberspace. A notable limitation of this paper is that classified solutions and sources cannot be mapped. Nevertheless, the resulting methods and tools that can be used for CW detection will likely overlap significantly with classified solutions.

2.0 CYBERSPACE – OPPORTUNITY FOR COGNITIVE WARFARE DETECTION

The primary focus of this paper is on opportunities provided by an overlap between cyber and cognitive warfare as depicted in Figure 1, as CW is strongly interrelated with cyberspace and can also be described as a "form of warfare that uses cyber tools" [1]. Nevertheless, physical means of influencing the human brain should not be excluded in its general understanding. Even terrorism can be considered a form of psychological or cognitive warfare with its indirect effects on the population, [3] but direct attacks on the target audience's brains are also a possible threat. Some sources argued that a possible cause of Havana syndrome, where diplomats experienced a range of symptoms impairing their cognitive functions, was a newly developed acoustic or microwave weapon [4]; [5]. While this explanation is unlikely based on clinical studies, [6]; [7] technologies with such capabilities are no longer sci-fi. Bearing that in mind, there will always be a set of CW tools outside cyberspace, which are out of the scope of this paper.

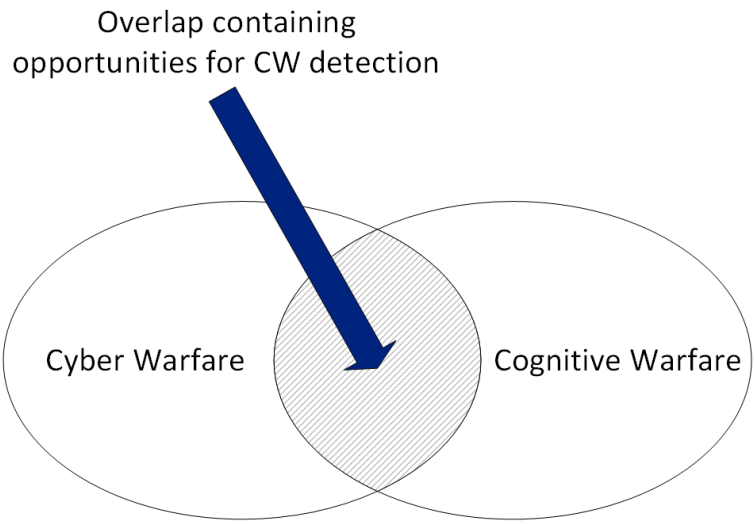

Figure 1: Cyber warfare and cognitive warfare overlap as foundation for CW detection.

3.0 CRITERIA FOR COGNITIVE WARFARE DETECTION TOOLS

There are two primary prerequisites for considering any detection tool for cyber-attacks as possibly useful for CW. First and foremost, the tool must adequately address CW-related phenomena. Tools for monitoring social media for disinformation campaigns could be useful, while distributed Denial of Service (DDoS) detection would be mostly irrelevant for CW. However, with broad definitions of CW,[1] it is also quite complicated to assess what data the tools should analyze and what the resulting indicators and warnings should be. Fortunately, NATO Allied Command Transformation published a more narrow and specific definition [8]:

> *Cognitive warfare integrates cyber, information, psychological, and social engineering capabilities. These activities, conducted in synchronization with other Instruments of Power, can affect attitudes and behaviour by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary.*

[1] Such as those listed in paper from Claverie and Du Cluzel in their paper "Cognitive Warfare": The Advent of the Concept of 'Cognitics' in the Field of Warfare" [1].

It is possible to derive several explicit and implicit constituents of CW that are crucial for detection tools. These are similar to Lasswell's still somewhat relevant theory of communication, which can be summarized as "Who?", "Says What?", "In What Channel?", "To Whom?", and "With What Effect?" [9], but with critical differences. With widespread social media, CW is much less of a unilateral, one-way street. Instead, the target audience can further spread the narratives, resulting in further potential reach and effects. This phenomenon is described as "participatory propaganda" and is tightly connected to the concept of CW [10]; [11]. I consider core constituents for the detection tools being the following:

1) Actor;
2) Methods;
3) Content;
4) Target audience(s).

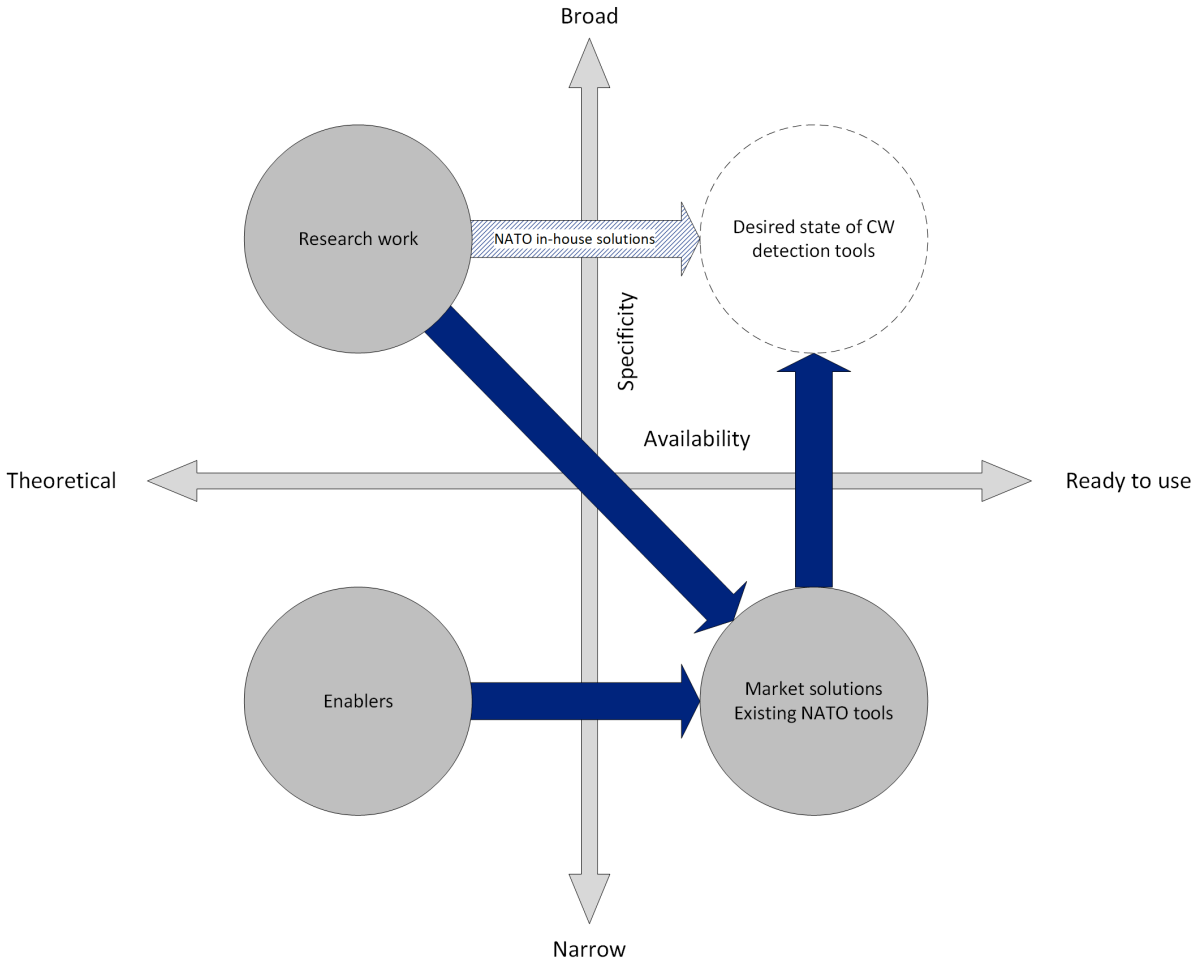

Figure 2: Visual representation of the desired end-state in regard to the detection tools for CW.

The second prerequisite is related to the complexity of cyberspace and the sheer amount of data to analyse. Any detection tool needs to be fully automated, which limits the scope primarily to solutions based on machine learning. NATO should focus on leveraging technologies for monitoring cyberspace that can provide warnings about CW operations in cyberspace and provide information on the four constituents mentioned above.

With the aforementioned prerequisites in mind, two important characteristics are influencing the desirability of reusing the tools for detecting CW in cyberspace – namely, their *specificity* and *availability*. Figure 2 is a visualization of *specificity* and *availability* on two axes, where the desired end state for tools lies in the top right quadrant – i. e., they have a broad range of use cases and are ready to be deployed.

3.1 Specificity

Tools and methods for cyber threat detection can be very specific in their focus. DDoS attack detection software solutions are an excellent example of very specific tools that cannot be easily used for different purposes without significant changes in the source code. On the other hand of the spectrum, there are more comprehensive (often only proposed) solutions for cyber threat detection. Most tools that are ready to be used are very narrow and specific. On the other hand, academic articles often come with innovative propositions for new tools and methods with numerous possible use cases. However, these are still theoretical and must be implemented in practice. Theoretical studies on very narrowly focused methods are also often published, but with the abundance of existing materials, the focus should be on the broadly useful methods among academic papers.

3.2 Availability

The tools and methods exist on a scale of availability between theoretical propositions and fully ready-to-deploy tools. In the case of NATO,[2] availability refers not only to the high *technology readiness level* [12] but also to the extent of control an actor-customer can have over the software itself. Organizations like NATO should not look for volatile solutions that might disappear from the market in the foreseeable future. The data needed for the tools must also be considered.

4.0 RESULTS

This section is split into three main parts. The first briefly discusses the two primary approaches to detection methods – ensemble and deep learning. The second deals with the top left quadrant of Figure 2 and can be summarised as “the methods.” The last part is focused on the lower right quadrant of Figure 2, discussing “the tools.” While the lower left quadrant of Figure 2 with “enablers” is generally important, it should not be the primary focus of NATO for CW detection, as narrow theoretical knowledge does not provide enough flexibility for new tools development.

4.1 Ensemble Learning & Deep Learning

The review of the most cited papers found by the search query has shown that detection methods benefit from being deployed in what is called *ensemble learning methods* or *deep learning*. Ensemble learning refers to a technique of combining two or more machine learning algorithms to achieve better and more accurate results [13]. On the other hand, deep learning refers to methods using artificial neural networks to teach the machine to extract information from raw data.

Mienye et al. argue that ensemble learning methods will be “instrumental in developing the next generation of state-of-the-art deep learning architectures” [13]. Most of the methods identified using the aforementioned query deal with either separate methods that can be used together as an ensemble learning method or with a proposed combination of methods. Several articles also argue for deploying deep learning algorithms for threat detection [14]; [15]; [16]. Ensemble learning can also combine multiple neural networks to achieve the advantages of both approaches [17]. Essentially, ensemble and deep learning are state-of-the-art approaches in all quadrants of Figure 2, and all methods and tools mentioned further are in some sense connected to them.

[2] And its individual member nations.

4.2 Broad & Theoretical – The Methods

Numerous studies deal with possible methods for cyber threat detection (see top left quadrant of Figure 2), and I cannot hope for an exhaustive list in the scope of this paper. I limited the dataset by using an advanced query, including several keyword combinations and excluding words that lead to unwanted results to find research articles as relevant to CW as possible. Only texts from recent years (since 2020) were included to restrict the results to relevant and novel research papers.

> *allintitle: detection (cyber-attack OR attack OR disinformation) -DDoS -physical -phishing -medical -microgrids -industrial*

Furthermore, a research article from Ahmetoglu and Das provided "a comprehensive review on detection of cyber-attacks," which served as another source for novel methods in the listed research articles [2]. Naturally, some articles cited other interesting research, resulting in a snowball effect.

4.2.1 Decision Tree & Random Forest

Decision tree algorithms can be used to classify vast volumes of data, which has applications in many fields and can be used to detect cyber-attacks [18]; [19]. Random forest is a method utilizing multiple decision trees randomly created from training data variables. The random forest method can be used in conjunction with other methods for anomaly detection, as demonstrated by Kumar et al. [20], but also discussed specifically regarding finding fake news by Khanam et al. [21]. Using decision trees and random forests for CW detection might not be the most novel approach, but it is worth exploring due to the high accuracy of algorithms used for related phenomena like disinformation and fake news.

4.2.2 Generative Adversarial Networks

Recently, generative adversarial networks[3] have been used to create so-called *deepfakes*, in many cases virtually unrecognizable by a human from real photos [22]. The model works as a competition between *discriminator* and *generator*, where the former tries to distinguish a real image and the latter tries to create one that is not recognizable from reality [22]; [23]. At first glance, the method seems to be more useful for *waging* CW than helping with defence, but it was listed among the possible detection tools by Ahmetoglu and Das [2] for a good reason. Generative adversarial networks can be used for detecting deepfakes, which can be a dangerous CW tool used to manipulate public opinion. Based on Goebbels' principles of propaganda, "credibility alone must determine whether propaganda output should be true or false," [24] which only strengthens the necessity to distinguish fake images and videos with high accuracy.

4.2.3 Shades of Truth

One of the more general "lessons learned" related to mis- and disinformation detection was listed by Hardalov et al., explaining that labelling information as binarily *true* or *false* is not sufficient and listing several studies that take this notion into account [25]; [26]; [27]; [28]. It is essential to understand that CW does not necessarily have to work with disinformation and blatant lies. On the contrary, the danger lies in spreading half-truths, mixing credible information and sources with unverifiable statements, or restricting information flow to the general public. Algorithms that work with more granular labelling on the truth-lie scale can be combined with other listed methods to achieve better results in CW detection.

[3] Essentially referring to networks that consists of generator – which creates, for example, images that resemble training data; and discriminator that tries to distinguish generated and real data. This way, the network learns to create and distinguish original content.

4.2.4 Social Network Analysis

One of the possible methods for future CW detection is social network analysis. Numerous possibilities and metrics for social network analysis [29] can potentially be utilized to detect CW in cyberspace. The aforementioned methods dealt primarily with threat detection itself, but in the context of defence against CW, it is also vital to identify key actors involved in adversarial operations. Furthermore, social network analysis can provide an ability to visualize the attacks' direction, scale, and other indicators, essentially helping in improving situational awareness.

4.2.5 Multimodal Content

It is said that *a picture is worth a thousand words*, and with technologies like deepfakes, CW detection requires focusing on multimodal content [25]. The information warfare surrounding the Russian invasion of Ukraine also saw a rise in what is now called *memetic warfare*, where both sides use short, visual content to influence public opinion, e. g., by discrediting the adversary. Researchers are already dealing with detecting propaganda and disinformation in multimodal content, focusing on issues ranging from propaganda in YouTube videos [30] to multilingual imagery content across multiple social media platforms [31]. To deal with a complex threat like CW, it is essential not to restrict the detection methods to textual evidence.

4.3 Narrow & Available – The Tools

The bottom right quadrant of Figure 2 primarily contains software solutions available on the market or specific tools built by actors like states and transnational organizations. The data gathering for this part of the paper was more unstructured, and I utilized informal discussions from the SAS-HFM-ET-FE *Early Warning System for Cognitive Warfare in Cyberspace* and other projects.

4.3.1 National Ecosystem for the Recognition and Analysis of the Information Effect Phenomena (NAAS)

One of the most promising projects that can be used for CW detection is the newly developed Lithuanian *National Ecosystem for the Recognition and Analysis of the Information Effect Phenomena*. The aim of the project is [32]:

> *...to train national and public security specialists and perform scientific activities involving information security, analysis of information and hybrid threats, integrated (Internet and kinetic) monitoring of the information space and analysis of potentially criminal content.*

NATO can benefit from member states sharing lessons learned from projects like Lithuanian NAAS, as CW is a pressing security threat, and attempting to build complex detection systems from scratch is not advisable.

4.3.2 The Europe Media Monitor (EMM)

The Joint Research Centre of the European Commission developed a system for monitoring tens of thousands of news websites and other public web pages [33]:

> *The high-volume stream of multilingual text articles enables research into multilingual natural language processing, and our research in text mining is investigating areas including multilingual topic mining, text classification, named entity recognition and the use of persuasion techniques in text.*

The system itself is not freely available, which only shows that increased cooperation between the EU and NATO is necessary to tackle the threat of CW. As the tool is relatively narrowly focused on textual processing, broadening its scope to multimodal content could benefit civil applications within the EU and

military within NATO. The tool has already proved useful during the COVID-19 pandemic for fact-checking [34]. Monitoring media for disinformation, propaganda, and other adversarial content is one of the first steps to increase the ability to combat CW.

4.3.3 Commercially Available Tools

A separate category of tools is the commercially available solutions ranging from complex monitoring systems to very narrow microservices – such as specialized pieces of code used for data scraping social media. Many such solutions are offered on the market, presenting an opportunity for NATO. Defence Innovation Accelerator for the North Atlantic (DIANA) was launched in 2022, promoting "interoperability among Allied forces and harness civilian innovation by engaging with academia and the private sector" [35]. DIANA can serve as a platform for smart-copying cyberspace monitoring solutions from large enterprises for CW detection. I do not directly encourage using any of the following examples, as they are just that – examples.

Of the commercially available solutions that could prove useful for CW detection, one stands out as a winner of the NATO ACT 2021 Innovation Challenge – *Belief3* suite of tools of Veriphix Inc. [36]. The solution is already closely related to CW through providing behavioral sciences insights, which makes it worth further investigation for specifically threat detection. The *Belief3* suite of tools, for example, includes solutions for analyzing the impact of messaging on a target audience.

LexisNexis Risk Solutions offers a variety of solutions, out of which their *ThreatMetrix* [36] might be the most useful for CW detection. Detection of bot attacks and users that use hidden proxies or VPNs are just a few of the tools provided within LexisNexis' *ThreatMetrix* solution that could help with the notoriously hard attribution in cyberspace.

Cisco Secure Network Analytics (Stealthwatch) provides network detection and response solutions [37] that could be modified to detect CW-related activities.

5.0 CONCLUSION – FROM METHODS TO TOOLS

Cooperation between NATO member states and all levels of society within the countries is necessary to deal with CW in the long term. Figure 2 shows that the desired state of detection tools for NATO lies in the top right quadrant that represents broad and working solutions. However, getting there is a matter of cooperation with academia, representing primarily the top left quadrant of Figure 2, and business, which lies in the lower right quadrant. Essentially, academia and business can play a crucial role in providing tools, technologies, and know-how for the detection of CW in cyberspace and NATO should draw from both areas to keep its technological edge. Academia can generate a plethora of methods, while businesses can transform them into working tools. The EU is also working on various tools for monitoring cyberspace, such as the aforementioned *Europe Media Monitor*, making increased collaboration between NATO and the EU important.

Methods listed in the top left quadrant of Figure 2 constitute the opportunity for NATO to develop in-house solutions for CW (see "Methods" in Table 1). However, it must be noted that it is challenging to transform theoretical methods into working solutions. For that reason, collaboration with companies that already offer some CW-related ways of monitoring cyberspace[4] (bottom right quadrant of Figure 2) is needed (see "Tools" in Table 1). The innovative theoretical knowledge primarily from academia can be implemented in practical solutions that will bolster NATO's defence against CW.

[4] From the commercial solutions, Veriphix's Belief3 suite of tools is probably the best example, as it already deals specifically with concepts related to CW.

Table 1: Promising tools and methods with potential use for Cognitive Warfare detection in cyberspace.

Methods (Broad & Theoretical)	Tools (Narrow & Ready to Use)
Generative Adversarial Networks	National Ecosystem for the Recognition and Analysis of the Information Effect Phenomena
Network Analysis	The Europe Media Monitor
Shades of Truth	Veriphix Inc. Belief3
Multimodal Content Analysis	LexisNexis ThreatMetrix
Decision Tree & Random Forest	Cisco Secure Network Analytics (Stealthwatch)

In conclusion, the primary concern of NATO in regard to CW detection should be a transformation from state-of-the-art methods to working tools. However, using even limited capabilities of existing tools available on the market or in the NATO member states is a feasible way of quickly increasing Allied capabilities in CW detection in cyberspace.

6.0 REFERENCES

[1] B. Claverie and F. Du Cluzel, "'Cognitive Warfare': The Advent of the Concept of 'Cognitics' in the Field of Warfare." NATO Collaboration Support Office, 2022, [Online]. Available: https://hal.science/hal-03635889/document

[2] H. Ahmetoglu and R. Das, "A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions," Internet of Things, p. 100615, 2022.

[3] A. Schmid, "Terrorism as psychological warfare," Democracy and Security, vol. 1, no. 2, pp. 137–146, 2005.

[4] J. C. Lin, "Microwave auditory effects among US Government personnel reporting directional audible and sensory phenomena in Havana," IEEE Access, vol. 10, pp. 44577–44582, 2022.

[5] R. Nelson, "Havana syndrome might be the result of energy pulses," Lancet, vol. 396, no. 10267, p. 1954, 2020.

[6] R. E. Bartholomew and R. W. Baloh, "Challenging the diagnosis of 'Havana Syndrome' as a novel clinical entity," Journal of the Royal Society of Medicine, vol. 113, no. 1, pp. 7–11, 2020.

[7] A. Friedman et al., "Havana syndrome among Canadian diplomats: brain imaging reveals acquired neurotoxicity," MedRxiv, p. 19007096, 2019.

[8] ACT NATO, "Cognitive Warfare: Strengthening and Defending the Mind." 2023, [Online]. Available: https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/

[9] H. Lasswell, "The structure and function of communication in society," in The communication of ideas, L. Bryson, Ed. New York: Harper & Bros, 1948, pp. 37–51.

[10] A. Wanless and M. Berk, "The audience is the amplifier: Participatory propaganda," in The Sage handbook of propaganda, P. Baines, N. O'Shaughnessy, and N. Snow, Eds. Sage, 2019, pp. 85–104.

[11] F. du Cluzel, "Cognitive warfare," Innovation Hub, NATO ACT, June – November 2020, [Online]. Available: https://www.innovationhub-act.org/sites/default/files/2021-01/20210113_CW Final v2 .pdf

[12] J. C. Mankins et al., "Technology readiness levels," White Paper April 1995.

[13] I. D. Mienye and Y. Sun, "A survey of ensemble learning: Concepts, algorithms, applications, and prospects," IEEE Access, vol. 10, pp. 99129–99149, 2022.

[14] M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, "A hybrid deep learning model for efficient intrusion detection in big data environment," Information Sciences, vol. 513, pp. 386–396, 2020.

[15] H. Zhang, Y. Li, Z. Lv, A. K. Sangaiah, and T. Huang, "A real-time and ubiquitous network attack detection based on deep belief network and support vector machine," IEEE/CAA Journal of Automatica Sinica, vol. 7, no. 3, pp. 790–799, 2020.

[16] C. Luo, Z. Tan, G. Min, J. Gan, W. Shi, and Z. Tian, "A novel web attack detection system for internet of things via ensemble classification," IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5810–5818, 2020.

[17] M. A. Ganaie, M. Hu, A. K. Malik, M. Tanveer, and P. N. Suganthan, "Ensemble deep learning: A review," Engineering Applications of Artificial Intelligence, vol. 115, p. 105151, 2022.

[18] B. Charbuty and A. Abdulazeez, "Classification based on decision tree algorithm for machine learning," Journal of Applied Science and Technology Trends, vol. 2, no. 01, pp. 20–28, 2021.

[19] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, "A novel hierarchical intrusion detection system based on decision tree and rules-based models," in 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2019, pp. 228–233.

[20] P. Kumar, G. P. Gupta, and R. Tripathi, "Toward Design of an Intelligent Cyber Attack Detection System using Hybrid Feature Reduced Approach for IoT Networks," Arabian Journal for Science and Engineering, vol. 46, pp. 3749–3778, 2021.

[21] Z. Khanam, B. N. Alwasel, H. Sirafi, and M. Rashid, "Fake news detection using machine learning approaches," in IOP conference series: materials science and engineering, 2021, vol. 1099, no. 1, p. 12040.

[22] M. Kumar, H. K. Sharma, and others, "A GAN-based model of deepfake detection in social media," Procedia Computer Science, vol. 218, pp. 2153–2162, 2023.

[23] M. Mirza and S. Osindero, "Conditional generative adversarial nets," arXiv Preprint arXiv1411.1784, 2014.

[24] L. W. Doob, "Goebbels' principles of propaganda," Public Opinion Quarterly, vol. 14, no. 3, pp. 419–442, 1950.

[25] M. Hardalov, A. Arora, P. Nakov, and I. Augenstein, "A survey on stance detection for mis-and disinformation identification," arXiv Preprint arXiv2103.00242, 2021.

[26] W. Y. Wang, "'Liar, liar pants on fire': A new benchmark dataset for fake news detection," arXiv Preprint arXiv1705.00648, 2017.

[27] G. Santia and J. Williams, "Buzzface: A news veracity dataset with facebook user commentary and egos," in Proceedings of the international AAAI conference on web and social media, 2018, vol. 12, no. 1, pp. 531–540.

[28] H. Rashkin, E. Choi, J. Y. Jang, S. Volkova, and Y. Choi, "Truth of varying shades: Analyzing language in fake news and political fact-checking," in Proceedings of the 2017 conference on empirical methods in natural language processing, 2017, pp. 2931–2937.

[29] L. Kirichenko, T. Radivilova, and A. Carlsson, "Detecting cyber threats through social network analysis: short survey," arXiv Preprint arXiv1805.06680, 2018.

[30] S. Abd Kadir, A. M. Lokman, and T. Tsuchiya, "Emotion and techniques of propaganda in YouTube videos," Indian Journal of Science and Technology, vol. 9, no. S1, 2016.

[31] M. Glenski, E. Ayton, J. Mendoza, and S. Volkova, "Multilingual multimodal digital deception detection and disinformation spread across social platforms," arXiv Preprint arXiv1909.05838, 2019.

[32] General Jonas Žemaitis Military Academy of Lithuania, "Development of the National Ecosystem for the Recognition and Analysis of the Information Effect Phenomena (NAAS)." 2020, [Online]. Available: https://www.lka.lt/news/360/618/Development-of-the-National-Ecosystem-for-the-Recognition-and-Analysis-of-the-Information-Effect-Phenomena-NAAS/

[33] European Commission, "Europe Media Monitor (EMM)." 2023, [Online]. Available: https://knowledge4policy.ec.europa.eu/text-mining/topic/europe-media-monitor-emm_en

[34] E. C. Joint Research Centre, "JRC to release AI tech for coronavirus fact-checkers." 2020, [Online]. Available: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/jrc-release-ai-tech-coronavirus-fact-checkers-2020-06-10_en

[35] NATO, "Defence Innovation Accelerator for the North Atlantic (DIANA)," 2023, [Online]. Available: https://www.nato.int/cps/en/natohq/topics_216199.htm

[36] Veriphix, "Belief3 tools." [Online]. Available: https://veriphix.com/belief3-tools

[37] LexisNexis Risk Solutions, "LexisNexis ThreatMetrix." [Online]. Available: https://risk.lexisnexis.com/products/threatmetrix

[38] Cisco, "Cisco Secure Network Analytics (Stealthwatch)." [Online]. Available: https://www.cisco.com/c/en_hk/products/security/stealthwatch/index.html