An Analysis of Cyberwarfare Attribution Techniques and Challenges

Clementine Swate, Siphesihle Sithungu and Khutso Lebea
University of Johannesburg, Auckland Park 2006, South Africa

clemmypontsho@gmail.com
siphesihles@uj.ac.za
klebea@uj.ac.za

Abstract. Identifying the source of cyber-attacks is crucial to ensuring cybersecurity. This study examines different attribution techniques, obstacles, and real-world examples in the context of cyber warfare. It explores challenges such as incorrect attributions, ethical concerns, legal barriers, and complexities in the digital environment. The discussed topic includes modern techniques such as malware analysis, network traffic study, digital forensics, and the implementation of AI/ML. These methods help improve cybersecurity and shape cyber warfare strategies. Case studies on the Standard Bank South Africa ATM fraud and the TransUnion South Africa cyber-attack illustrate the importance of attributing cyber incidents, especially with global cyber criminals. The analysis emphasizes the need for a comprehensive approach that takes into account legal, technical, ethical, and geopolitical considerations relevant to the evolution of computing and cyber warfare. It stresses the need for cybersecurity tools enhancement and global cooperation. The study pairs attribution challenges with techniques to deepen our understanding of threats. It underlines the need for ongoing cybersecurity research and adaptation, sustained innovation, and collaboration to fortify global cyber defenses.

Keywords: Cyberwarfare · Malware Analysis · Cyberattacks · Digital Forensics · Geopolitical Analysis · Open-Source Intelligence (OSINT)

1. Introduction

Technological advancements have revolutionized warfare in modern times. Cyberwarfare, an online form of fighting, is a new threat that is difficult to detect due to its complex and deceptive nature. As internet connectivity expands and more things connect, individuals and institutions become increasingly vulnerable to major cyberattacks. Therefore, it is crucial to determine the responsibility for these attacks, a process known as attribution.

The concept of cyberwarfare refers to cyber-attacks that are supported or associated with a government and have military or political goals (AlShaer & Rahman, 2015). These attacks are a major worldwide security concern as they can have significant impacts on a country's infrastructure, economy, and safety. Whether it involves spying, disruption, or damage, correctly identifying the origin of cyberattacks is essential to maintain global stability, discourage malicious actors, and respond effectively to such threats.

This paper delves into the intricate realm of cyberwarfare attribution, encompassing a range of methods and approaches used to identify individuals or entities responsible for cyberattacks. The framework for comprehending cyberwarfare attribution comprises technical, behavioral, linguistic, geopolitical, and state-of-the-art artificial intelligence (AI) and machine learning methodologies, each playing an important role in the intricate and difficult quest for attribution (DiMaggio, 2022). While it is crucial to understand and advance these techniques, they also present challenges and limitations.

Misattribution, which involves wrongly accusing an entity or nation of a cyberattack, remains a persistent concern. Furthermore, the ethical implications surrounding attribution, particularly in the context of nation-states and cyber-conflict, pose complex dilemmas that require careful consideration.

2. Attribution techniques in Cyberwarfare

Identifying the source of cyberattacks is a challenging and multifaceted undertaking that necessitates the use of a range of methods and approaches. This section examines different attribution methods, highlighting their significance in the context of cyber warfare.

2.1 Technical Analysis

The identification of cyberattacks largely depends on technical analysis, which entails a meticulous examination of digital evidence and technical elements that may have been left behind (Goel & Nussbaum, 2021). With this type of investigation, important information about the source of the attack can be revealed. The following subcategories offer a comprehensive comprehension of different technical analysis methods.

2.1.1 Malware Analysis:

Cyberattacks often use malicious software, such as viruses, worms, Trojans, and ransomware. To identify the source of an attack, investigators perform malware analysis. This involves breaking down and reverse engineering the malicious code to determine its unique characteristics, features, and any ties to known malware groups (DiMaggio, 2022). By identifying these details, investigators can connect an attack to a specific group, individual, or state actor.

2.1.2 Network Traffic Analysis:

The process of network traffic analysis involves closely examining the communication between an attacker and a target system. It includes monitoring network packets, traffic patterns, and identifying malicious command and control (C2) channels (Ferrag et al., 2023). Through analyzing these aspects, analysts can uncover important information about the attacker's location, infrastructure, and possible affiliations. This information can be used to develop effective strategies for preventing future attacks.

2.1.3 Digital Forensics:

Digital forensics is a method of gathering and analyzing digital proof from compromised systems. This process helps investigators to reconstruct the timeline of the attack, identify the initial attack vector, and trace the actions of the attacker within the victim's environment (AlShaer & Rahman, 2015). It plays a crucial role in comprehending how an attack was carried out and identifying those who may be responsible for it.

2.2 Behavioral Analysis

Behavioral analysis is a critical element in the field of cyberwarfare attribution. Its primary focus is to understand the tactics, techniques, and procedures (TTPs) used by threat actors during cyberattacks (DiMaggio, 2022). By carefully examining the behavioral patterns and operational methods of attackers, analysts can create profiles or fingerprints that help attribute attacks to specific threat groups, nation-states, or individuals. The key aspects of behavioral analysis include:

2.3.1 Tactics, Techniques, and Procedures (TTPs):

Threat actors make strategic and operational choices known as Tactics, Techniques, and Procedures (TTPs) in their cyber operations. TTPs include the different stages of an attack, such as initial reconnaissance, intrusion, data exfiltration, or system disruption (Goel & Nussbaum, 2021). Attack vectors are the different ways in which attackers can access a target system or network. These methods consist of phishing, exploiting vulnerabilities, and social engineering. On the other hand, malware deployment techniques involve studying how malware is delivered, activated, and maintained inside the target environment. This includes the usage of droppers, command and control servers, and persistence mechanisms. Evasion and stealth techniques are the methods used to avoid detection and keep a low profile within the victim's infrastructure. These techniques involve using encryption, obfuscation, and living-off-the-land tactics.

2.3.2 Attack Timeline Reconstruction:

The reconstruction of attack timelines plays a crucial role in analyzing behaviors for attributing cyberwarfare. In this process, the events sequence during a cyberattack is pieced together, like putting together a digital puzzle. This method is invaluable for comprehending the attacker's actions, motivations, and decision-making. It is crucial to reconstruct the timeline of an attack accurately. This involves dividing the attack into different stages, including initial reconnaissance, exploitation, privilege escalation, data exfiltration, and impact. It is essential to understand how the attacker interacts with the victim's systems. This could involve lateral movement through the network, privilege escalation, or communication with command-and-control servers. Furthermore, it is crucial to analyze the attacker's decision-making process and motivations. It helps to identify whether their actions are driven by financial gain, espionage, or political objectives.

2.3 Linguistic Analysis

In the complex world of cyberwarfare attribution, linguistic analysis plays a crucial role. This technique involves analyzing the language, coding style, and behavioral patterns used by threat actors in their digital activities. By

examining these linguistic aspects, analysts can gain valuable insights into the identities and affiliations of malicious entities (Kapsokoli, 2023). The key elements of linguistic analysis include:

2.3.3 Language Markers

Language markers are linguistic indicators in digital artifacts like code or documents that give clues about the actor's origin (Kapsokoli, 2023). To identify the language used by an attacker, one can carefully analyze the language used in emails, chat conversations, and forum postings related to cyber operations. One can also determine the attacker's place of origin or specific community they belong to by examining various language variants and regional dialects. By analyzing idiomatic terms and cultural allusions used in an attacker's communication, it is possible to infer their cultural background and experiences.

2.3.4 Coding Style Analysis

Coding style analysis examines unique patterns and idiosyncrasies in code and software development practices. This analysis is particularly relevant when examining malicious code. Coding conventions refer to the unique formatting options, naming conventions, and coding practices used in software code or malware that can indicate a specific person or organization Examining debugging artifacts, errors, or code flaws unique to a developer or team helps identify code source. Furthermore, analyzing the language and content of code comments and documentation can reveal insights into the developer's personality or history.

2.3.5 Comments and Developer Habits

Software developers and hackers often exhibit consistent habits and practices that can be used to identify them. For instance, determining the attacker's working hours and time zone can help reveal their location. Identifying the programming languages, tools, or frameworks that attackers prefer can be connected to well-known developer practices. Reusing code or methodologies in multiple attacks may indicate the consistent work of a single actor or group.

Linguistic analysis is a robust and effective tool for attribution, as it offers an exclusive insight into the human elements behind cyber operations. By scrutinizing linguistic hints, coding styles, and developer habits, analysts can link apparently unconnected attacks and create a more comprehensive profile of threat actors, thus improving the accuracy of attribution.

2.4 Geopolitical Analysis

When trying to identify cyber attackers in the context of cyber warfare, geopolitical analysis is essential. This approach goes beyond the digital realm to examine the broader geopolitical motivations, alliances, and affiliations of those who pose a threat (AlShaer & Rahman, 2015). Geopolitical analysis involves looking at the following key aspects.

2.4.1 Motivations of Threat Actors

Understanding the motives behind a cyberattack is crucial in determining attribution. The objectives of the attacker, which range from espionage to influencing political events, can provide insight into their identity or affiliation. Cyberattacks can have different motivations, such as political goals, financial gains, or cyber espionage. State-sponsored actors are often involved in attacks that aim to influence elections, overthrow governments, or achieve specific political objectives. Cybercriminal organizations are usually responsible for attacks that seek to make money, such as ransomware campaigns or theft of intellectual property. On the other hand, nation-states involved in cyber-espionage operations are seeking intelligence for strategic purposes. (Ferrag et al., 2023).

2.4.2 Alliances and Affiliations

Nations and threat actors often operate within alliances or affiliations. Geopolitical analysis considers the relationships that may underpin a cyber operation. When multiple countries form cooperative agreements or strategic alliances, they may work together on cyber operations. These types of attacks are the responsibility of the member countries within the alliance. Threat actors who carry out assaults on behalf of nation-states are known as proxy actors. Identifying these proxies can help link the attacks to their main financiers.

2.4.3 Open-source Intelligence and Collaborative Intelligence

In the world of cyberwarfare attribution, open-source intelligence (OSINT) and collaborative intelligence play a crucial role. OSINT is the practice of gathering publicly available information from sources such as social media, forums, news outlets, and government reports (Kapsokoli, 2023). Collaborative intelligence helps in promoting cooperation among security organizations, governments, and private sector entities. It enables them to share information and expertise, which is essential in the fight against cybercrime. The use of Open-Source Intelligence (OSINT) techniques can provide several benefits, such as corroborating evidence by keeping an eye on the online activities of threat actors or their associated groups, thus offering more proof of attribution. Collaborative intelligence can allow for better information sharing among groups to identify and counteract cyberthreats by combining resources and expertise.

2.5 AI and Machine Learning

The fields of cyberwarfare and attribution have been greatly enhanced by the emergence of artificial intelligence (AI) and machine learning (ML). These tools enable data analytics, pattern recognition, and automation to increase the precision and efficiency of attribution efforts. AI and ML are utilized in various ways, including linguistic analysis and behavioral pattern recognition. This section will explore the applications and implications of AI and ML in cyberwarfare attribution.

2.5.1 Linguistic Analysis Through NLP

Natural Language Processing (NLP) is a subfield of AI that focuses on computer-human language interaction. NLP plays a significant role in attributing cyberwarfare. Language Recognition is a technique that can help reduce the number of potential cyber attackers by using AI-powered natural language processing models to automatically recognize and detect the language used in cyberattack conversations (Goel & Nussbaum, 2021). Another useful NLP technique is Sentiment Analysis which can analyze an attacker's tone and sentiment to reveal information about their intentions. Stylometric Analysis is a method that uses AI to identify distinctive language patterns in writing style, vocabulary, and grammatical quirks. These patterns can be used to connect assaults to certain writers or organizations (Kapsokoli, 2023).

2.5.2 Behavioral Pattern Analysis Using ML Algorithms.

Behavioral pattern analysis involves using machine learning algorithms to identify patterns in the behavior of threat actors. Machine learning (ML) models can be used to identify possible security risks by detecting odd or suspicious activity within a system or network. By using previous data to identify attack signatures, machine learning algorithms can be trained to link future attacks to identified threat actors through attack signature matching. Machine learning can help classify and attribute new threats by creating behavioral profiles of different threat groupings through group profiling.

3. Challenges and Limitations

While the techniques and methodologies for cyberwarfare attribution are advancing, the field is rife with complexities and challenges. Accurately attributing cyberattacks to their source can be elusive, and there are limitations and ethical implications that must be considered. This section delves into the hurdles faced in the attribution process.

3.1 Misattribution

Misattribution is a major concern in cyberwarfare due to the risk of attributing a cyberattack to the wrong source, which can have serious consequences. Misattribution can occur for various reasons. False flags refer to intentional actions by threat actors to mislead investigators by planting false clues or using deceptive techniques to deflect blame (Mohamed et al., 2023). Attackers often use compromised infrastructure to conceal their origins, making it difficult to trace attacks. In some cases, investigators may choose not to reveal the identity of an attacker, even if they are certain about it, due to classified information or geopolitical considerations (Mohamed et al., 2023). The reuse of attack tools and malware by different threat groups can cause confusion, making it difficult to accurately attribute cyber-attacks (Ngulu, 2022). Addressing misattribution requires a high degree of expertise, extensive data, and a cautious approach to avoid making hasty accusations.

3.2 Ethical Implications

Ethical considerations are crucial in the process of attributing cyberattacks. The act of attribution can have significant consequences, and there are ethical dilemmas that need to be addressed (Pahi & Skopik, 2019).

Misattribution can lead to innocent entities being wrongly accused, which can have serious consequences. Public attribution, in some cases, can escalate conflicts, potentially leading to further retaliation in the cyber or physical realm. Balancing the need for transparency in disclosing cyber threats with the need to protect sensitive sources and methods poses ethical dilemmas. Moreover, the collection and analysis of personal data, even for attribution purposes, may infringe upon individual privacy and civil liberties. It is important to take these factors into account when dealing with cyber threats to ensure fair and just outcomes.

3.3 Attribution in the Digital Fog

The digital realm's anonymity and obfuscation make attribution difficult. Threat actors use advanced techniques to remain hidden. Attackers may hide their true locations by routing activities through proxy servers and anonymization tools. The use of botnets composed of compromised devices complicates attack tracing due to multiple, dispersed sources. Attackers often alter their infrastructure by using dynamic IP addresses and changing tactics to make it difficult to trace them. The attribution process is difficult due to incomplete and rapidly changing information.

3.4 Legal and Political Impediments

It can be difficult to determine who is responsible for cyberwarfare due to the complexity of the legal and political landscape surrounding attribution. This involves dealing with a range of legal issues, the process of attributing cyberattacks across borders often involves complex legal procedures, leading to difficulties in determining the applicable legal jurisdiction. Establishing globally accepted legal standards for cyber attribution remains a work in progress and is a challenge to be addressed. Geopolitical factors such as diplomatic relations and national interests can significantly influence the attribution decision-making process.

Legal and political considerations can impede attribution, affecting its efficacy. The following table outlines how different cyberwarfare attribution challenges align with specific techniques discussed in the paper. It provides a clearer understanding of how these challenges are addressed or associated with specific attribution methodologies and approaches.

Table 1: Alignment of Challenges and techniques

Challenges in Cyberwarfare Attribution	Associated Techniques
Misattribution	Malware Analysis Network Traffic Analysis Digital Forensics TTPs (Tactics, Techniques, Procedures)
Ethical Implications	Linguistic Analysis Geopolitical Analysis
Attribution in the Digital Fog	AI and Machine Learning Digital Forensics
Legal and Political Impediments	Geopolitical Analysis

4. Case Study

The details of the case studies presented in this paper are based on publicly available information from news reports and official statements from the organizations involved. The selection of the Standard Bank South Africa ATM fraud and the TransUnion South Africa cyberattack as case studies were random, without specific criteria guiding their selection. These cases were chosen to provide illustrative examples of cyber incidents and to demonstrate the complexities of attribution, rather than being selected based on predetermined criteria or characteristics. We will discuss the cyber-attack involving Standard Bank South Africa and a significant ATM fraud in Japan. This incident highlights the intricacies of attributing cyberattacks and emphasizes the importance of robust cybersecurity in the financial sector.

4.1 The Cyberattack in Japan

In May of the year 2021, a large-scale cyberattack occurred in Japan involving the fraudulent withdrawal of significant sums of money from ATMs. Approximately 100 individuals used forged Standard Bank credit cards to withdraw over R250 million (¥1.8 billion) from 1,400 ATMs across Tokyo and other regions in Japan in under three hours. The incident amounted to an estimated loss of about R300 million for Standard Bank, a major financial institution based in South Africa (Moyo, 2022).

Response and Ongoing Investigation

In response to the incident, Standard Bank took measures to mitigate the impact, secure its systems, and address the vulnerabilities exploited by the attackers. South African officials launched an investigation into the incident and took steps to collaborate with Japanese law enforcement agencies.

Attribution Outcome

The specific attribution outcome remained uncertain at the time of this case study. The complexity of attributing such large-scale cyberattacks, coupled with the use of fraudulent cards and international coordination, can make identifying the perpetrators challenging (Qusai & Sadkhan, 2021).

Table 3 and Table 4 provide a detailed breakdown of techniques employed and challenges faced in the context of the Standard Bank South Africa cyberattack in Japan, reflecting the specific methods and difficulties encountered.

Table 2: Suggested techniques that could be applied in the case study.

Techniques Used in Case Study	References
Malware Analysis	Investigation into the malicious code found within the compromised ATM systems in Japan to understand its characteristics and possible connections to known malware groups.
Network Traffic Analysis	Examination of communication patterns between the attackers and Standard Bank's systems to identify the origin and nature of the attack.
Digital Forensics	Collection and analysis of digital evidence from the hacked bank's system to reconstruct the attack's timeline and uncover the perpetrators' actions.
TTPs (Tactics, Techniques, Procedures)	Identification of specific attack methodologies, such as unauthorized access and fraudulent withdrawals in Japan, examining the methods used in the cybercrime.
Linguistic Analysis	Scrutiny of language markers in communications between the attackers, e.g., emails or messages, potentially revealing the identities or affiliations of the cybercriminals.
Geopolitical Analysis	Investigation into the motivations and implications behind the attack, possibly for financial gain, cyber-espionage, or part of an organized criminal group.
AI and Machine Learning	Utilization of AI and ML algorithms to detect patterns and anomalies in the cybercrime behavior, aiding in identifying the attackers.

Table 3: Challenges applicable to the case study

Challenges in Case Study	References
Misattribution	Risk of incorrectly attributing the cyberattack to a specific entity or nation due to the utilization of proxy servers and misleading clues to deceive investigators.
Ethical Implications	Consideration of potential impacts on innocent parties, risk of further escalation, and concerns about individual privacy during the cybercrime investigation.
Attribution in the Digital Fog	Difficulty in tracing the attackers due to the use of anonymizers, botnets, and rapidly changing infrastructure, hindering the attribution process.
Legal and Political Impediments	Complexity in determining legal jurisdiction and establishing globally accepted standards for cyber attribution amidst geopolitical and diplomatic considerations.

4.2 The Cyberattack on TransUnion South Africa

In the recent TransUnion South Africa cyberattack, a hacker group known as N4aughtysecTU claimed responsibility for breaching the credit bureau's systems. According to the claims made, this group, allegedly from Brazil, asserted access to 54 million personal records of South Africans and demanded a 15 million ransom (R223 million) for the release of the compromised data. The group stated it gained access to the TransUnion server using a client's credentials and had been operating within the system since 2012 without detection (Reporter, 2016).

Response and Ongoing Investigation Following the breach, TransUnion took immediate measures, suspending the compromised client's access, engaging cyber security and forensic experts, and initiating an investigation into the incident. Certain services were taken offline as a precautionary step, and TransUnion South Africa has since resumed these services. The company is working closely with law enforcement and regulatory authorities to address the issue.

Attribution Outcome From the statement given by Transunion in the newspaper article the actual attribution of the cyberattack remained uncertain. The intricate challenges of linking the breach to a specific group or nation, coupled with the hacker group's claims and the complexities of international cyber investigations, presented significant challenges in identifying the responsible actors.

Table 4 and Table 5 provide a detailed hypothetical breakdown of techniques employed and challenges faced in the context of the TransUnion South Africa cyberattack, reflecting the specific methods and difficulties encountered in this scenario.

Table 4: Suggested techniques that could be applied in the case study.

Techniques Used in Case Study	Reference to Case Study
Malware Analysis	Examination of the systems to detect potential malware or intrusion mechanisms used to access and exploit TransUnion's servers.
Network Traffic Analysis	Analysis of the traffic patterns to identify unauthorized access and data exfiltration from the compromised server.
Digital Forensics	Collection and examination of digital evidence from the breached server to reconstruct the attack timeline and identify the attackers.
TTPs (Tactics, Techniques, Procedures)	Identification of the specific methodologies used by the hacker group, including how they gained access through authorized client credentials and navigated undetected.
Linguistic Analysis	Scrutiny of any communication or messages exchanged between the hacker group and TransUnion regarding the extortion demands and potential threats.
Geopolitical Analysis	Investigation into the origins and affiliations of the hacker group, who claim to be from Brazil, and their threats against South African entities.
AI and Machine Learning	Utilization of AI algorithms for anomaly detection, particularly to identify potential weak points or overlooked security vulnerabilities in TransUnion's systems.

Table 5: Challenges applicable to the case study

Challenges Applicable to Case Study	Reference to Case Study
Misattribution	Risk of potentially attributing the attack to a particular group or nation (Brazil) without concrete evidence or due to misleading statements by the hacker group.
Ethical Implications	Consideration of the potential exposure of sensitive personal data, the company's response to extortion demands, and the threat of further data exposure.
Attribution in the Digital Fog	Difficulty in tracing the hacker group due to their claim of operating undetected in TransUnion's systems since 2012 and the information leakage threats.
Legal and Political Impediments	Complexity in determining the hacker group's actual location and holding them accountable across international jurisdictions for cyberattacks.

5. Conclusion

The conclusion drawn from this study underscores the intricate challenges inherent in the realm of cyberwarfare attribution, shedding light on its pivotal role within the broader landscape of cybersecurity. While the issue of misattribution, wherein the wrong entity is identified as the perpetrator of an attack, looms as a notable concern, the detailed examination of the Standard Bank South Africa ATM fraud and the TransUnion South Africa cyberattack case studies provides valuable insights into the multifaceted nature of attributing cyber incidents. Through these case analyses, it becomes evident that navigating the complexities of attribution demands a holistic and collaborative approach that encompasses legal, technical, ethical, and geopolitical considerations.

Moreover, the findings underscore the imperative for continuous research and adaptation in the field of cybersecurity. As cyber threats continue to evolve and adversaries employ increasingly sophisticated tactics, there exists an ongoing need to innovate and refine strategies for bolstering global defenses. By emphasizing the significance of sustained innovation and collaboration, it advocates for the development of adaptable frameworks that can effectively mitigate the ever-evolving cyber threat landscape.

In essence, the conclusions drawn from this research underscore not only the challenges inherent in cyberwarfare attribution but also the imperative for concerted efforts towards enhancing cybersecurity practices. Through a nuanced understanding of attribution challenges and a commitment to ongoing research and collaboration, stakeholders can better position themselves to safeguard against emerging cyber threats and uphold the integrity of digital ecosystems worldwide.

References

Al-Shaer, E. and Rahman, M.A., 2015. Attribution, temptation, and expectation: A formal framework for defense-by-deception in cyberwarfare. *Cyber Warfare: Building the Scientific Foundation*, pp.57-80.

DiMaggio, J. (2022). *The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime*. No Starch Press.

Ferrag, M. A., Kantzavelou, I., Maglaras, L., & Janicke, H. (Eds.). (2023). *Hybrid Threats, Cyberterrorism and Cyberwarfare*. CRC Press.

Goel, S. and Nussbaum, B., 2021. Attribution across cyber-attack types: network intrusions and information operations. *IEEE Open Journal of the Communications Society*, *2*, pp.1082-1093.

Kapsokoli, E. (2023). *Cyberterrorism: A New Wave of Terrorism*. https://doi.org/10.1201/9781003314721

Mohamed, N., Almazrouei, S. K., Oubelaid, A., Ahmed, A. A., Jomah, O. S., & Aghnaiya, a. (2023, May). *Understanding the Threat Posed by Chinese Cyber Warfare Units. In 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, pp. 359-364. IEEE.

Ngulu, J.M., 2022. Efficacy of International Humanitarian Law in Addressing Cyber Warfare as a New Weapon Technology: An Analysis of the Gaps and Way Forward. *The Eastern African Law Review*, *45*(1).

Pahi, T., & Skopik, F. (2019, July). *Cyber attribution 2.0: Capture the false flag. In Proceedings of the 18th European Conference on Cyber Warfare and Security* (ECCWS 2019), pp. 338-345.

Qusai, A. D., & Sadkhan, S. B. (2021, August). *Cyberwarfare Techniques: Status, Challenges and Future trends. In 2021 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, pp. 124-129. IEEE.

Wandugi, L. K. (2020). *Attribution and state responsibility in cyber warfare: a case study of the not Petya attack.*

Moyo, A. (2022). *Breaking: Credit bureau TransUnion hacked.* ITWeb. Available at https://www.itweb.co.za/content/o1Jr5Mx9BVjqKdWL. Accessed: 01 October 2023.

Reporter, S. (2016). *Standard Bank Scam: R300-million ATM heist ups the ante*. The Mail & Guardian. Available at [https://mg.co.za/article/2016-05-27-r300-million-atm-heist-ups-the-ante/]. Accessed: 01 October 2023