Attribution Challenges in the Era of Cyber Warfare: Unraveling the Identity of Cyber-Attackers

Rafeak M Salem Abu Alead [1]
mr_aboalead@hotmail.com
ALI AMHMED AB ALTALIBE [2]
Ali.atalpie@gmail.com

Abstract:

Cyber warfare has emerged as a prominent threat in our interconnected world, introducing a paradigm shift in the nature of conflict. As adversaries exploit the anonymity afforded by the digital realm, attributing cyber-attacks becomes a formidable challenge. This research paper, titled "Attribution Challenges in the Era of Cyber Warfare: Unraveling the Identity of Cyber-Attackers," delves into the complexities surrounding the identification of those responsible for cyber threats. The paper explores the technological, geopolitical, and legal dimensions of attribution, highlighting the limitations of current methodologies and the implications of false attributions on international relations. By fostering interdisciplinary collaboration, the research aims to contribute insights that can enhance the accuracy and credibility of attributing cyber-attacks in this dynamic landscape.

Keywords:

(Cyber Warfare, Attribution Challenges, Digital Anonymity, Interdisciplinary Collaboration)

1- Higher lnstitute of Medical Technologies, Sabratha, Libya
2- Higher lnstitute of Medical & Tochnolgies - Aljomil

Introduction:

In an age dominated by digital connectivity and technological advancement, the landscape of warfare has extended beyond traditional battlefields to encompass the vast realm of cyberspace. The rise of cyber warfare has ushered in a new era of conflict where state and non-state actors engage in sophisticated attacks, exploiting the vulnerabilities of interconnected systems. Amidst this digital battleground, one of the most perplexing and consequential challenges faced by cybersecurity experts is the attribution of cyber-attacks.

The research paper, "Attribution Challenges in the Era of Cyber Warfare: Unraveling the Identity of Cyber-Attackers," delves into the intricate web of complexities surrounding the identification of those responsible for cyber threats. In an environment where anonymity and obfuscation are integral components of the attacker's toolkit, attributing cyber-attacks to specific entities becomes a formidable task**(Rid, etal. 2015).** This paper seeks to unravel the multifaceted challenges inherent in the attribution process, shedding light on the technological, geopolitical, and legal dimensions that contribute to the enigma.

As the frequency and sophistication of cyber-attacks continue to escalate, the need to accurately attribute these incidents becomes paramount. The paper explores the limitations of current attribution methodologies, the impact of false attributions on international relations, and the evolving tactics employed by cyber adversaries to remain in the shadows. By dissecting the various layers of this intricate puzzle, the research aims to contribute valuable insights into the development of more effective and reliable attribution mechanisms.

In navigating the uncharted waters of cyber warfare attribution, the research recognizes the importance of interdisciplinary collaboration, bringing together experts in computer science, international law, and geopolitics. By fostering a comprehensive understanding of the challenges at hand, the paper strives to pave the way for innovative solutions that can enhance the accuracy and credibility of attributing cyber-attacks in this ever-evolving landscape. As we confront the complexities of the digital age, unraveling the identity of cyber-attackers **(Tsagourias, etal, 2020)**emerges as a critical endeavor in safeguarding the integrity of our interconnected world.

Research Problem:

The research problem addressed in the study revolves around the intricate and persistent challenges associated with attributing cyber-attacks to their perpetrators. In the dynamic landscape of cyber warfare, identifying the entities behind malicious activities remains a formidable task. The anonymity, obfuscation tactics, and rapidly evolving methodologies employed by cyber adversaries pose significant hurdles for cybersecurity experts and agencies attempting to ascertain responsibility for cyber incidents. The lack of a comprehensive and foolproof attribution framework hampers the effectiveness of cyber defense strategies, making it imperative to delve into the complexities of cyber attribution.

Research Objectives:

- **Explore Current Attribution Challenges:**

Objective: To comprehensively examine and understand the existing challenges that impede accurate attribution of cyber-attacks. This includes an analysis of the techniques employed by cyber adversaries to conceal their identities, exploit vulnerabilities, and evade detection.

- **Assess Technological Limitations in Attribution:**

Objective: To evaluate the technological constraints hindering precise attribution in the era of cyber warfare. This involves an in-depth examination of existing attribution methodologies, their limitations, and the need for technological advancements to overcome these challenges.

- **Examine Geopolitical and Legal Dimensions:**

Objective: To investigate the geopolitical factors influencing cyber attribution and the legal implications surrounding the identification of cyber-attackers. This includes an exploration of how international relations and legal frameworks contribute to or hinder the attribution process.

- **Develop Interdisciplinary Solutions:**

Objective: To propose interdisciplinary approaches and collaboration models that bring together expertise from computer science, international law, and geopolitics. The aim is to foster a holistic understanding of attribution challenges and devise innovative solutions that address the multifaceted nature of the problem.

- **Evaluate Impacts of False Attributions:**

Objective: To analyze the repercussions of false attributions in the context of cyber warfare. This involves studying case scenarios where inaccurate attributions have occurred, understanding the impact on international relations, and highlighting the importance of precision in attribution.

- **Contribute Insights for Future Attribution Mechanisms:**

Objective: To provide valuable insights and recommendations for the development of more effective and reliable attribution mechanisms. This

includes proposing advancements in technology, international collaboration frameworks, and legal frameworks to enhance the accuracy and credibility of attributing cyber-attacks.

By addressing these research objectives, the study aims to contribute to the ongoing discourse on cyber warfare attribution, providing a nuanced understanding of the challenges and proposing viable solutions to unravel the identity of cyber-attackers in an era marked by sophisticated digital threats.

Related Work:

In the realm of cyber warfare and attribution challenges, a substantial body of research has emerged, addressing various facets of this complex landscape. The existing literature encompasses studies focusing on technological advancements, geopolitical implications, and interdisciplinary approaches to mitigate the challenges posed by cyber-attacks.

literature Review

1. **Technological Advancements in Attribution:**

   Unmasking Cyber Adversaries in the Era of Digital Warfare

   (Ghose, etal.,2016). navigates the intricate landscape of cyber threats and the challenges associated with attributing cyber-attacks. In the context of this study, the discussion on technological advances in attribution takes a different trajectory, emphasizing the transformative potential of individual-level data in the realm of cybersecurity.

   Similar to the advancements witnessed in digital advertising, the increasing availability of individual-level data marks a paradigm shift in the standards for measurability and accountability in cyber warfare attribution. This paper draws parallels by highlighting the significance

of leveraging massive datasets for a nuanced understanding of cyber-attack attribution.

The study's approach mirrors the sophistication seen in digital advertising research. It utilizes a massive individual-level dataset, mirroring the comprehensive nature of digital advertising datasets. The unique features of this dataset include insights into the actual viewability of impressions and the duration of exposure to cyber threats at the individual-user level. These features become pivotal in distinguishing this research from prior work in the field.

Employing a quasi-experimental design, the study employs advanced statistical methods, such as difference-in-differences, matching techniques, and instrumental variable approaches. These methodologies are crucial for controlling both observable and unobservable confounders, mirroring the meticulous approach adopted in digital advertising research.

The empirical findings of the study reveal that, akin to the influence of display advertising on consumer behavior, cyber exposure significantly impacts users' propensity to search for cyber adversaries and understand their tactics. Consumers engage in both active search, where they actively gather information, and passive search, relying on external information sources. The research establishes statistically and economically significant effects of cyber exposure on increasing the effectiveness of cybersecurity measures, contributing to the overarching goal of mitigating cyber threats.

Furthermore, the study delves into the temporal aspect, demonstrating that the duration of exposure to cyber threats plays a pivotal role. The

longer the exposure, the more likely users are to engage in direct search behaviors, such as directly identifying cyber adversaries, rather than indirect ones, like relying on generic search inquiries.

In essence, this research bridges the gap between technological advances in attribution witnessed in digital advertising and the complex landscape of cyber warfare. By adopting similar principles and methodologies, the study contributes to the development of a framework for evaluating cyber attribution effectiveness, constituting a crucial stepping stone towards causally addressing the digital attribution problem in the context of cybersecurity.

2. **Geopolitical Perspectives on Cyber Warfare:**

(Huskaj, etal. 2023,) is an examination of the current landscape of digital geopolitics, an area of great interest in national digital strategies and scholarly research. Despite this interest, there is a notable absence of a comprehensive review of the scholarly literature on digital geopolitics. Using a computational literature review method, the researchers identified 124 articles in a scientific database, which were eventually narrowed down to 120 articles with author and abstract information. The study reveals a significant increase in research output from 2015 onwards, covering 53 distinct topics in the dataset. The analysis highlights the prevailing focus on the areas of technology, information and geo security, with less emphasis on political and health-related aspects. The findings provide valuable insights into the evolving landscape of digital

geopolitics, highlighting the most cited articles and prominent publishing venues in the field.

The research delves into the challenges of attribution in the context of cyber warfare, with a particular focus on uncovering the identity of cyber attackers. As the era of cyber warfare evolves, understanding the complexities associated with attributing cyber-attacks has become increasingly critical. The study aims to contribute to current knowledge by highlighting the complex dynamics of cyber attribution, addressing the challenges posed by anonymity and evolving tactics used by cyber attackers. By revealing the identity of these perpetrators, the research seeks to strengthen cybersecurity measures and strategies to mitigate the impact of cyber threats on organizations and countries.

This section explores the geopolitical dimensions of cyberwar, with the aim of providing a comprehensive understanding of the intersection between international relations and digital conflict. Analyzing geopolitical perspectives on cyberwar involves examining how nation-states navigate and strategize in the cyber domain, taking into account issues such as digital espionage, cyberattacks, and the role of technology in shaping geopolitical power dynamics. The study aims to contribute valuable insights into the evolving landscape of cyberwarfare from a geopolitical perspective, providing a nuanced perspective on the ways in which states engage in and respond to cyber threats in the context of global politics.

The aim of the study was **(Sophie, etal. 2023).** This research aims to explore and emphasize the importance of using social media data in

gaining critical insights into the cyber conflict between Russia and Ukraine. The study underscores the unprecedented ability of social media platforms to provide real-time information dissemination, enabling timely tracking and analysis of cyber incidents. By leveraging a wide range of user-generated content, including eyewitness accounts and multimedia evidence, the research seeks to leverage these invaluable resources to confirm and contextualize cyberattacks. In addition, the study aims to use social media data to understand public sentiment, propaganda dissemination, and emerging narratives. The overarching goal is to provide a comprehensive analysis of the critical role of social media-based cyber intelligence in understanding cyber threats to Russia during the ongoing Russia-Ukraine conflict. The research presents an innovative multidimensional cyber intelligence framework that uses advanced monitoring tools and NLP algorithms to automatically generate cyber intelligence reports.

Based on the use of Twitter data spanning October 13, 2022 to April 6, 2023, with 37,386 tweets from 30,706 users in 54 languages, the study provides the first detailed multilingual analysis of the Russia-Ukraine cyber crisis. The research focuses on four cyber dimensions: geopolitical, social, economic, targeted victim, psychological and societal, and national priorities and concerns. Using advanced technologies such as language detection, translation, sentiment analysis, TF-IDF, LDA, Porter Stemming, n-grams, and others, the study provides automated cyber intelligence for Russia and Ukraine. The findings highlight the challenges of harnessing reliable social

media-based cyber intelligence, emphasizing the importance of such analyzes in understanding and responding to cyber conflicts.

In the field of cyber warfare, this study delves into the attribution challenges prevailing in the current era. Specifically, the research focuses on uncovering the identity of cyber attackers and identifying the complexities associated with attributing cyber attacks to specific entities. As the cyber threat landscape evolves, understanding and overcoming attribution challenges is essential for effective cybersecurity measures. The study contributes to existing knowledge by highlighting the complex dynamics of cyber attribution, addressing issues related to anonymity and sophisticated tactics used by cyber attackers. By revealing the identity of these perpetrators, the research aims to enhance cybersecurity strategies and countermeasures to mitigate the impact of cyber threats on organizational and national security.

Multidisciplinary cooperation in the field of cybersecurity:

This section explores the critical role of interdisciplinary collaboration in cybersecurity. Recognizing that cyber threats often transcend traditional disciplinary boundaries, the study delves into how collaboration across diverse fields such as computer science, law, psychology, and international relations can contribute to more robust cybersecurity measures. The research aims to highlight the benefits and challenges of multidisciplinary collaboration in addressing complex cyber threats, while emphasizing the need for a comprehensive and collaborative approach to address the multifaceted nature of cybersecurity challenges.

3. **Interdisciplinary Collaboration in Cybersecurity:**

Objectives of the study:

(**Hamburg, etal. 2023)** research aims to address the multi-faceted challenges in cybersecurity by focusing on the need for a broader pool of cybersecurity professionals, both prepared employees and employers. Recognizing the complex nature of cybersecurity issues, the study aims to investigate interdisciplinary knowledge gaps within this field. The aim is to emphasize the importance of social, legal, ethical, socio-psychological, technical, economic and managerial elements in cybersecurity activities, and how professionals, managers and employees may lack comprehensive interdisciplinary knowledge. Additionally, the study highlights the critical role of diversity and inclusion in the cybersecurity workforce, with the goal of fostering a diverse talent pool to enhance decision-making and problem-solving in the face of cyber threats. The research anticipates that education and training, along with approaches such as Universal Design for Learning (UDL) and Design Thinking (DT), can contribute significantly to addressing these challenges.

The paper presented research findings on cybersecurity training, showcasing the application of interdisciplinarity, diversity and inclusion through the Erasmus+ project called InCyT (Interdisciplinary Cyber Training). Within the framework of this project, a two-year training and mentoring program for SMEs is being developed, along with a digital platform. The study incorporates Design Thinking (DT) as an iterative, human-centered problem-solving approach and integrates it with Universal Design for

Learning (UDL) to enhance the attractiveness and effectiveness of cybersecurity education and training. The principle of Universal Design for Learning (UDL) is implemented by providing learners with multiple means of representation, expression, and participation. The goal is to accommodate diverse learners, including people with disabilities or social challenges, ensuring equal access to training. Through phases inspired by Waloszek (2012), the research emphasizes the importance of reflective online journals, support of mentors, and engagement in interdisciplinary projects to foster empathy among learners and address real-world cybersecurity needs.

4. **False Attributions and Their Implications:**

In the realm of cybersecurity, understanding the identity and motives of cyber-attackers is a formidable challenge, akin to unraveling a complex puzzle. One of the intricate aspects contributing to this challenge is the phenomenon of false attributions. This article delves into the implications of false attributions and their impact on our comprehension of cyber threats.

1. Unmasking the False Consensus Effect:

study **(Van der Pligt, J. 1984)** involving 1,056 participants, sought to explore attitudes, knowledge, and behavior concerning various environmental issues. The findings revealed a cognitive bias known as the "false consensus effect," where observers tend to perceive a consensus regarding the prevalence of their own behavioral choices. Interestingly, this bias extended across a spectrum of behaviors. It's noteworthy that this phenomenon was not linked to participants' trait inferences about the typical person making a specific choice.

The research indicated that neither the perceived commonness of responses nor the participants' own behavioral choices adequately explained the observed differences in attributional inferences. Notably, participants exhibited a tendency to make more extreme and confident trait ratings for evaluatively positive behavior, regardless of their own choices. This aligns with the proposal by**(L. Ross ,1977)** suggesting that individuals tend to make more extreme ratings about dissimilar others when they rate their own choices unfavorably compared to the alternative. The implications of these findings on understanding the false consensus effect in the context of cyber threats are discussed, offering insights into evaluative and motivational mechanisms.

2. Distorted Perceptions in Cyber Attribution:

Evidence from four distinct studies underscores that social observers commonly fall prey to a "false consensus" regarding the perceived commonness of their own responses. This bias extends to social inferences, where raters tend to view responses similar to their own as common and less revealing of personal dispositions. Conversely, responses differing from those of the observer are seen as uncommon and more telling of the actor's characteristics **(Ross, etal, 1977).**

These findings emerged from both hypothetical scenarios and real conflict situations, indicating the robust nature of the false consensus effect. The article explores the implications of these cognitive biases on social perception within the cybersecurity domain. Furthermore, it proposes cognitive and perceptual mechanisms that might contribute to distortions in perceived consensus and corresponding biases in cyber attribution processes.

3. Impact of Performance Feedback on Attributional Processes:

In an exploration of organizational humanitarian behaviors, a study **(Bachrach, ., etal, 2001)**.involving 95 teams of business students engaged in a labor-scheduling simulation. The teams received feedback regarding their performance, either false negative, false positive, or neutral. The results suggested that the perception of organizational humanitarian behavior within workgroups, specifically helping behavior and civic virtue, may be influenced by the nature of performance feedback received.

Interestingly, negative feedback played a more pivotal role in shaping attributional processes than positive feedback. The implications of these findings on understanding how feedback shapes perceptions of cyber threats and cyber-attackers are discussed, shedding light on the intricate interplay between feedback mechanisms and attributional processes in the cybersecurity landscape.

5. **Addressing Technological Challenges:**

In the landscape of cyber warfare, the imperative to unmask the identity of cyber attackers has never been more pressing. Technological advancements, while integral to the evolution of cybersecurity, bring forth a myriad of challenges in attributing cyber threats to their true originators.

The relentless prevalence of cyber threats mirrors the challenges encountered in the medical realm, where diseases like HIV, TB, and malaria persist, alongside emerging infectious diseases such as influenza A (H7N9), Ebola, and MERS. These threats create formidable obstacles for patient care, especially in resource-limited settings (RLS). The implementation of advanced diagnostic technologies in such settings remains hindered by economic constraints. **(Wang, etal., 2016).** Advances in addressing technical

challenges of point-of-care diagnostics in resource-limited settings.The pursuit of simple and cost-effective point-of-care (POC) diagnostics has become a focal point, aiming to facilitate early diagnosis and treatment monitoring in non-laboratory environments.

Despite concerted efforts from material science, biomedical engineering, and nanotechnology, significant technical challenges persist in the development of POC diagnostics for RLS. This summary encapsulates the ongoing struggles in overcoming these challenges and offers a comprehensive review of the latest advances in the field. It underscores the critical need for innovative solutions that transcend economic constraints, echoing the analogous challenges faced in the cyber realm.

The Intersection of Technology and Society:

In the context of cyber-attacks, the intricate dance between technology and society unfolds as a central theme. Contemporary theories often lean towards technological determinism, portraying technology as a force that shapes social, cultural, and economic change. However, this perspective is under scrutiny within the realm of social studies of science and technology (STS). Scholars in this field challenge the deterministic view and emphasize that technology is a socio-technical product, intricately woven into the fabric of its creation and utilization.

This**(Wajcman, etal. 2002)** article delves into the evolution of STS, highlighting its critique of technological determinism and presenting key concepts that underscore the interdependence of technology and society. It asserts that these realms are not separate but mutually constituted, offering a nuanced understanding that accounts for the materiality of social relations

and the influence of objects. Moreover, the article explores the contributions of scholars specializing in gender and technology, enriching both STS and feminist theory. The insights gained from this perspective resonate with the complex interplay between technology and the actors involved in cyber-attacks.

Shifting Paradigms in Power Systems:

In an era where variable inverter-based renewable energy sources are reshaping electric power systems, parallels can be drawn between the challenges faced in the energy sector and those encountered in cyber warfare. This article examines the global shift toward renewable generation technologies and its implications for power systems. As the dominance of renewable energy technologies increases, questions arise regarding the operation of these systems.

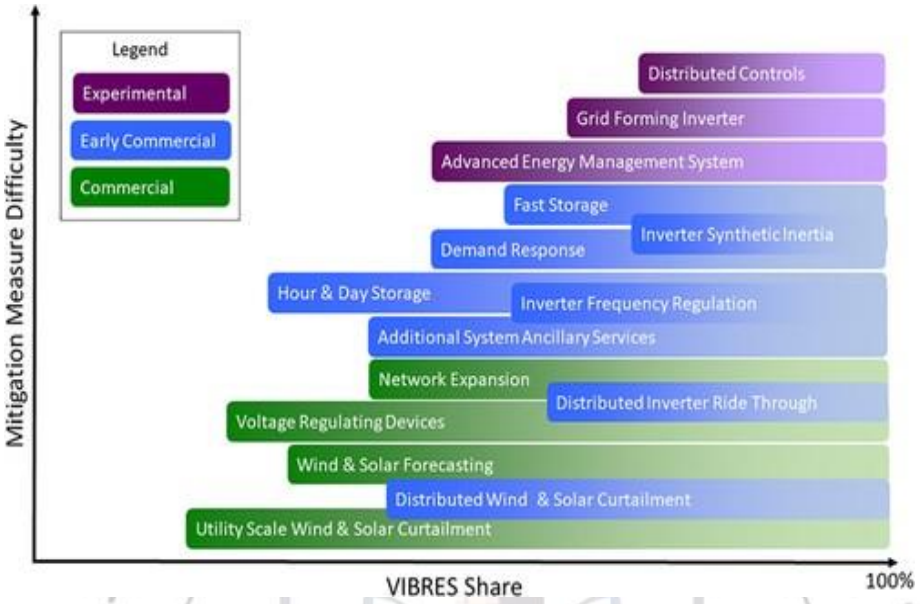

Figure (2)**(Hodge, etal., 2020)**

The review outlines the challenges posed by the rising share of variable inverter-based renewable energy sources and provides an overview of proposed mitigation strategies. The categorization under Wind Power, Energy Systems Economics, and Energy Infrastructure highlights the interdisciplinary nature of the challenges faced **(Hodge, etal., 2020)** This examination of the energy landscape serves as a metaphorical reflection of the evolving complexities in attributing cyber threats, where adapting to shifting paradigms is imperative for resilience.

In conclusion, the challenges presented in these diverse fields underscore the universal struggle in navigating complex technological landscapes. Whether in healthcare diagnostics, the sociotechnical fabric of society, or the transformation of power systems, addressing technological challenges

requires innovative solutions and a holistic understanding of the intricate interplay between technology and its broader context. Similarly, in the cyber realm, unraveling the identity of cyber-attackers demands a multidisciplinary approach and a nuanced comprehension of the evolving threat landscape.

Empirical Findings

In the dynamic landscape of cyber warfare, the quest to decipher the identities of cyber-attackers stands as a formidable challenge. This exploration delves into empirical findings that shed light on the complexities surrounding the attribution of cyber threats, emphasizing the intricate nature of unraveling the identity of those behind these malicious activities.

- Contextualizing the Challenge:

The prevalence of cyber threats has escalated in tandem with technological advancements, creating an intricate web of challenges for cybersecurity professionals. Empirical research becomes a crucial tool in dissecting these challenges and understanding the nuances that characterize the attribution process in the realm of cyber warfare.

- Dynamic Nature of Cyber Threats:

Empirical findings underscore the dynamic and evolving nature of cyber threats. These findings reveal a landscape where cyber-attackers adapt, innovate, and exploit vulnerabilities in unpredictable ways. Understanding the methodologies employed by these adversaries requires a nuanced examination of empirical data, enabling cybersecurity experts to adapt their strategies and defenses accordingly.

- Attribution Challenges Explored:

Empirical evidence sheds light on the multifaceted challenges associated with attributing cyber-attacks to specific entities. The anonymity afforded by the digital realm, coupled with sophisticated tactics such as false flag operations, presents hurdles in pinpointing the true originators. Empirical studies scrutinize the intricacies of these challenges, providing insights into the psychological and technical aspects that cloak cyber-attacker identities.

- Human Factor in Attribution:

Beyond the technological intricacies, empirical findings emphasize the human factor in attribution challenges. Cyber-attackers often exploit human vulnerabilities through tactics like social engineering, further complicating the identification process. Understanding the psychological aspects behind these attacks becomes paramount, as empirical data reveals patterns and trends that inform strategies for countering such manipulative tactics.

- Advancements in Attribution Techniques:

While challenges persist, empirical research highlights advancements in attribution techniques. The integration of artificial intelligence, machine learning, and behavioral analytics emerges as promising avenues for improving the accuracy and efficiency of identifying cyber-attackers. These empirical insights inform ongoing efforts to develop robust frameworks that leverage technological innovation for enhanced attribution capabilities.

- Implications for Cybersecurity Policy:

Empirical findings contribute to the formulation of cybersecurity policies by providing evidence-based insights. Understanding the intricacies of cyber-attacker behavior, motives, and tactics informs the development of proactive

measures and response strategies. The empirical foundation enables policymakers to craft resilient frameworks that adapt to the evolving threat landscape.

In the era of cyber warfare, empirical findings serve as the cornerstone for unraveling the identity of cyber-attackers. As technological landscapes evolve, so do the challenges associated with attribution. This exploration emphasizes the need for ongoing empirical research to inform the development of effective strategies, technologies, and policies aimed at countering the elusive nature of cyber threats. The journey to unravel the identity of cyber-attackers continues, guided by the insights gleaned from empirical investigations into this complex and ever-evolving domain.

Conclusion

In conclusion, the exploration of attribution challenges in the era of cyber warfare reveals a complex and dynamic landscape. Cyber threats continue to evolve, demanding constant adaptation from cybersecurity experts. Unraveling the identities of cyber-attackers proves to be a multifaceted task, shaped by the intricate interplay of technological advancements and human vulnerabilities.

The human element introduces a psychological dimension, with social engineering tactics and manipulation playing a significant role in cyber-attacks. Despite these challenges, technological advancements in artificial intelligence and machine learning offer promising prospects for refining attribution techniques. The implications for cybersecurity strategy highlight the necessity of resilience and adaptability.

Collaborative defense emerges as a crucial aspect, emphasizing the need for shared knowledge among international cybersecurity communities. As we

conclude this exploration, the shadows in the cyber realm persist, underscoring the ongoing commitment required to understand, innovate, and collaborate in the relentless pursuit of cybersecurity.

References:

1. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1-2), 4-37.
2. Tsagourias, N., & Farrell, M. (2020). Cyber attribution: technical and legal approaches and challenges. European journal of international law, 31(3), 941-967.
3. Sufi, F. (2023). Social Media Analytics on Russia–Ukraine Cyber War with Natural Language Processing: Perspectives and Challenges. Information, 14(9), 485.
4. Huskaj, G. (2023, February). Digital Geopolitics: A Review of the Current State. In International Conference on Cyber Warfare and Security (Vol. 18, No. 1, pp. 152-161).
5. Hamburg, I. (2023). SUPPORTING INTERDISCIPLINARITY, DIVERSITY AND INCLUSION IN CYBERSECURITY. In INTED2023 Proceedings (pp. 106-111). IATED.
6. Van der Pligt, J. (1984). Attributions, false consensus, and valence: Two field studies. Journal of Personality and Social Psychology, 46(1), 57.
7. Ross, L., Greene, D., & House, P. (1977). The "false consensus effect": An egocentric bias in social perception and attribution processes. Journal of Experimental Social Psychology, 13(3), 279-301. https://doi.org/10.1016/0022-1031(77)90049-X. Link to the article
8. Ross, L., Greene, D., & House, P. (1977). The “false consensus effect”: An egocentric bias in social perception and attribution processes. Journal of experimental social psychology, 13(3), 279-301.

9. Bachrach, D. G., Bendoly, E., & Podsakoff, P. M. (2001). Attributions of the" causes" of group performance as an alternative explanation of the relationship between organizational citizenship behavior and organizational performance. Journal of Applied Psychology, 86(6), 1285.
10. Wang, S., Lifson, M. A., Inci, F., Liang, L. G., Sheng, Y. F., & Demirci, U. (2016). Advances in addressing technical challenges of point-of-care diagnostics in resource-limited settings. Expert review of molecular diagnostics, 16(4), 449-459.
11. Wajcman, J. (2002). Addressing technological change: The challenge to social theory. Current sociology, 50(3), 347-363.
12. Hodge, B. M. S., Jain, H., Brancucci, C., Seo, G. S., Korpås, M., Kiviluoma, J., ... & Kroposki, B. (2020). Addressing technical challenges in 100% variable inverter-based renewable energy power systems. Wiley Interdisciplinary Reviews: Energy and Environment, 9(5), e376.
13. Marciano, M., Bohmayr, W., & Klier, O. (2022, June 15). A Geopolitical Lens for Cyber Resilience.