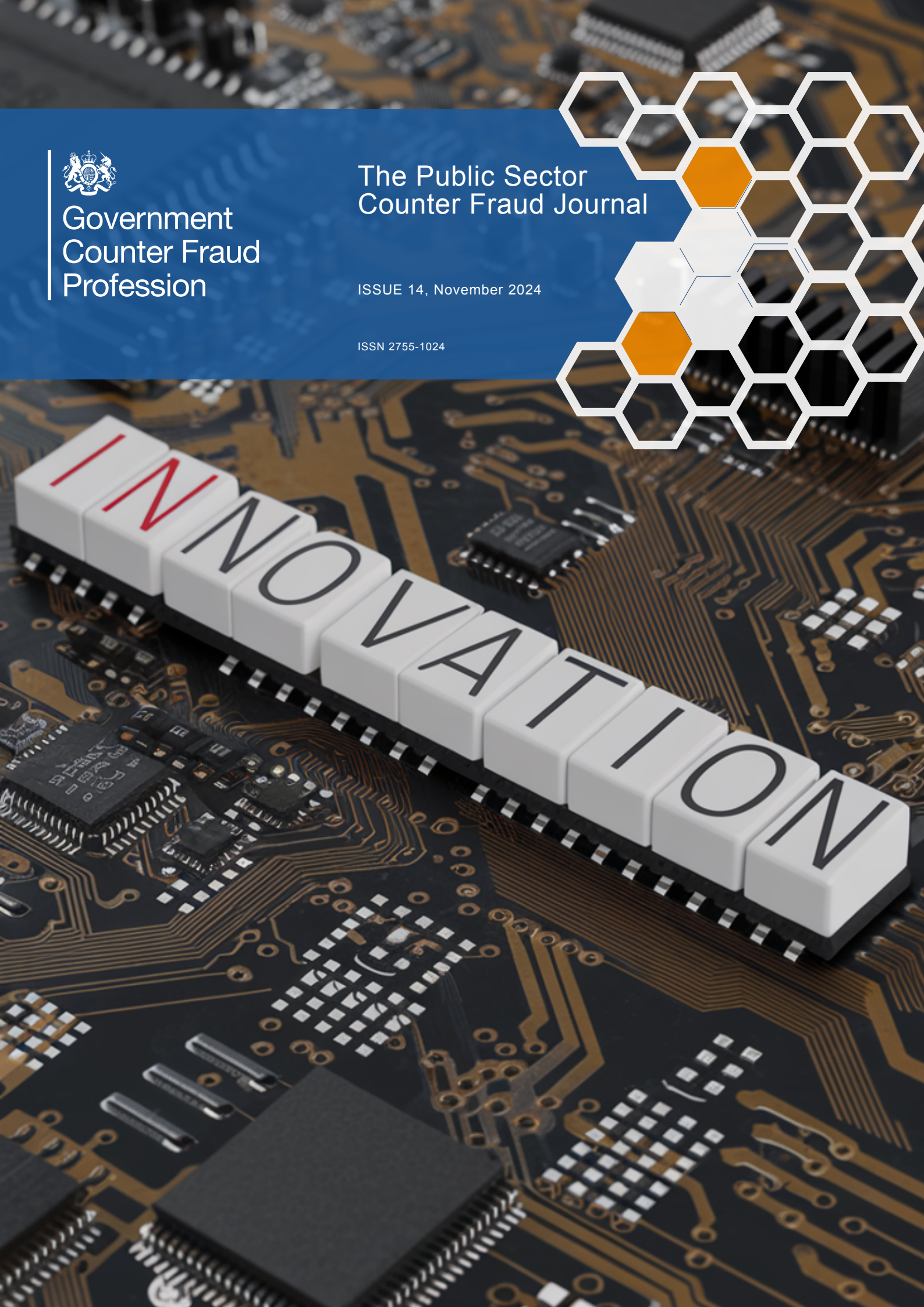
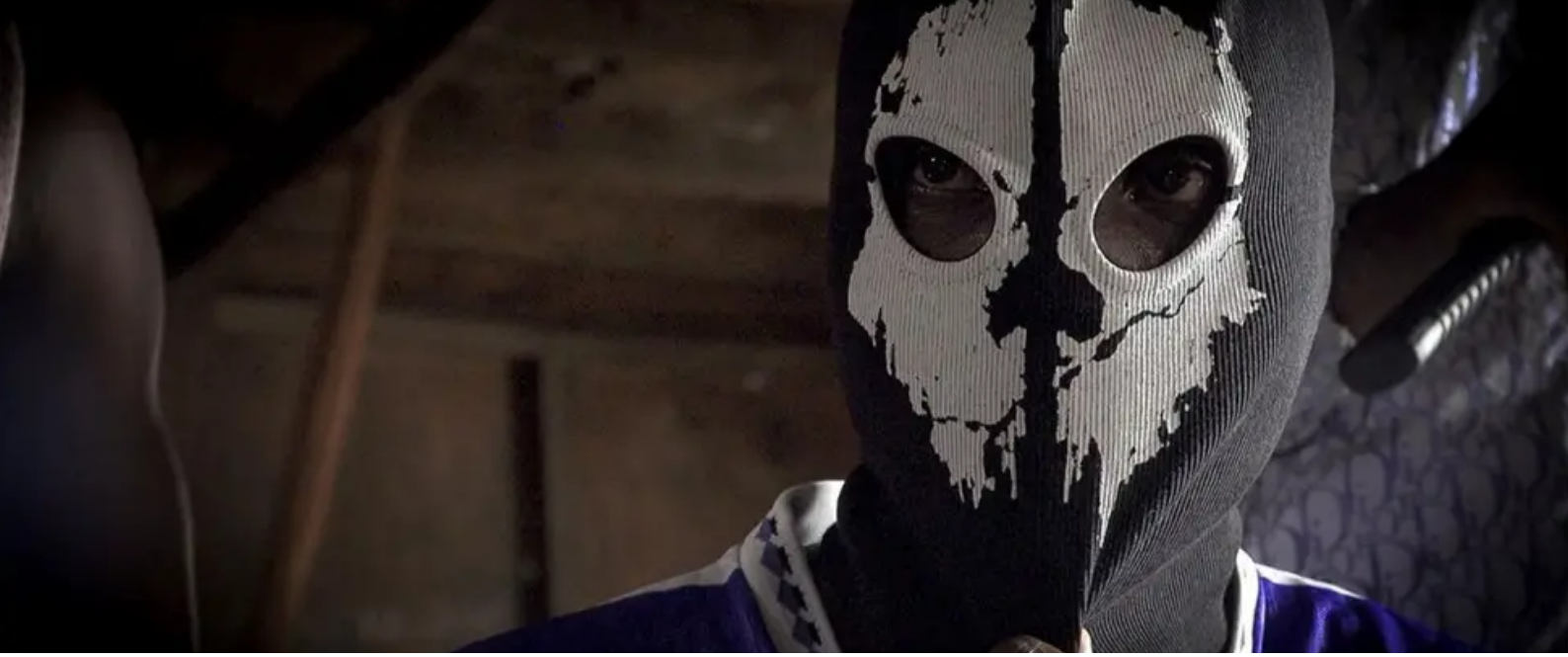


Government Counter Fraud Profession

The Public Sector Counter Fraud Journal

ISSUE 14, November 2024

ISSN 2755-1024



Assessing Cybercrime Syndicates: Understanding 'Black Axe' Confraternity and Cybercriminal Networks in Business Email Compromise (BEC) Scams

"Suleman Lazarus, PhD, is a Visiting Fellow at the London School of Economics and Political Science (LSE) and serves as an Associate Editor for the Association for Computing Machinery (ACM) journal "Digital Threats: Research and Practice."

Dr Suleman Lazarus

Introduction

Cybercrime is a global threat affecting both public and private sectors. Business email compromise (BEC) is one of the most advanced and lucrative forms of cybercrime, exploiting vulnerabilities in corporate email systems to facilitate unauthorised financial transactions.[1] Organisations worldwide suffer substantial losses from these attacks. Notable examples include:

•**Evaldas Rimasauskas** was sentenced in 2019 for defrauding Facebook and Google of $121 million by using a fake company, "**Quanta Computer.**"[2]
•In 2015, cybercriminals impersonated third-party vendor employees and tricked **Ubiquiti** into losing $46.7 million.[2]
•In 2019, a hacker deceived an employee at **Toyota Boshoku Corporation**, resulting in a $37 million transfer from the company's European subsidiary.[2]
•**Obinwanne Okekewas** sentenced in 2021 for defrauding victims of $11 million in a BEC scheme.[2]
•In 2022, **Ramon Olorunwa Abbas (a.k.a. Hushpuppi)** was sentenced for BEC scams and conspiring to deceive a law firm into transferring $922,857.76.[3]

In 2023, BEC scams resulted in $50 billion in losses in the United States,[4] with the United Kingdom potentially facing similar figures. Comparably, Interpol identified groups like "Black Axe" as key players in global online fraud, targeting both public and private sectors..[5] Despite high-profile arrests in Ireland, the UK, and Canada, efforts to address the root causes of these syndicates remain inadequate..[1],.[5] This article explores the connection between Black Axe and BEC scams, providing insights into how public sector organisations can better combat these sophisticated criminal networks.

Expert Witness Experience: The Case of Black Axe and BEC Schemes

As an expert witness in a case against a Black Axe member and alleged 'leader' of a cybercriminal syndicate in a Western country, I gained valuable insight into Black Axe's involvement in cybercrime. Through interviews with the accused, each lasting approximately four hours, and actionable intelligence provided by the authority, I found no evidence of a rigid hierarchy dictating roles or compensation within BEC operations.[1] Instead, the structure was decentralised and fluid, fostering collaboration, adaptability, and specialisation.[1] BEC's operational model presents significant challenges to law enforcement, who often interpret these scams through the traditional hierarchical lens of organised crime.[1] This misalignment blurs the understanding, handling, and dismantling of these networks.[1]

Value of the Research

This study offers a unique perspective on the inner workings of cybercriminal networks like Black Axe, specifically their involvement in BEC. While media reports, such as those from The Toronto Sun,[6] have linked Black Axe to cybercrime, no prior academic research has gathered direct testimonies from convicted members involved in these schemes, making my findings both rare and highly valuable to the counter-fraud community. The research provides real-world insights into how these networks operate, recruit, and adapt. For public sector organisations and law enforcement, understanding these operational details directly from those involved can strengthen investigative techniques and counter-fraud measures, particularly across international borders. This research offers unique insights into Black Axe's operational dynamics and role in BEC scams. The findings are organised into three key areas:

1. Role Flexibility and Challenges in Visualising Networks

While BEC scammers within the Black Axe network may use threats of violence to assert control, their operational model contrasts the rigid hierarchies of traditional organised crime syndicates. In traditional crime groups (e.g., the Yakuza in Japan, the Bratva in Russia, the Triads in China, and the Mafia in Italy), roles are strictly defined with clear chains of command. In contrast, BEC schemes operate through fluid, decentralised, unpredictable networks with highly adaptable and shifting roles. Members frequently transition between tasks, such as recruiters, managers, or conduits, based on the specific needs of each scam or 'transaction'. This flexibility allows the group to exploit various opportunities, making it harder for investigators to link individuals to specific roles. This adaptability makes these networks far harder to understand than conventional organised crime's more structured, predictable frameworks. Cybercriminal networks' elusive, dynamic nature complicates law enforcement efforts, leading to potential inaccuracies or misattribution of roles. How can we improve intelligence-gathering to map elusive networks like Black Axe?

2. Global Reach and Transnational Dimensions

Black Axe's BEC scams represent a transnational phenomenon with far-reaching intentions and consequences. Their worldwide network enables them to target businesses and public sector organisations across borders. Arrest and imprisonment alone are often insufficient to disrupt this complex, multi-jurisdictional web of financial fraud. Some authorities mistakenly assume that imprisonment marks the conclusion of an investigation. Re-examining tapped phone data by experts with knowledge of local epistemologies, linguistic codes, and contextual artefacts may uncover hidden network components often missed by foreign observers, offering deeper insights into transnational cybercriminal networks.

Given that most internet scam-related arrests by the Economic and Financial Crimes Commission (EFCC) in Nigeria involve Southerners rather than Northerners,[7] and with Black Axe originating in the South and having a global membership primarily consisting of Southerners, it is essential to contextualise the group's activities within broader regional dynamics. These dynamics continue to shape both the roles criminal actors play in transnational cybercrime and the recruitment pathways within Black Axe. Southerners with community ties to existing members benefit from established mentorship networks and employment opportunities within these organisations. This creates a recruitment cycle where individuals from the same region are drawn into such schemes, guided by those already familiar with the nitty-gritty of scamming entrepreneurship. Local sociocultural dynamics have transnational consequences. Research indicates that some Afrobeats singers, whose songs are widely available on popular platforms like Spotify, Apple Music, SoundCloud, Deezer, and Pandora, glamorise BEC offenders like 'Hushpuppi' and collaborate in laundering illicit funds.[8] The influence of music celebrities amplifies the social acceptance of internet scams. Likewise, the distinction between "Yahoo Boys" (internet fraudsters) and "Yahoo Men" (corrupt politicians) in Nigeria is blurred, as both groups share similar expertise and advance their careers through fraud.[9] How can regional sociocultural dynamics be leveraged to better understand transnational cybercriminal networks?

3. Cryptocurrency and Money Laundering

Cryptocurrencies, like Bitcoin, play a pivotal role in Black Axe's BEC operations, offering relative anonymity and fluidity in laundering illicit funds. Unlike traditional financial systems, cryptocurrencies transcend geographical and jurisdictional boundaries, enabling seamless cross-border transactions with minimal oversight.[10] This decentralised nature complicates efforts to trace illicit gains, as transactions circumvent banking channels and regulatory frameworks. The pseudonymity afforded by cryptocurrency further conceals criminals' identities, making it harder for law enforcement to pinpoint key actors.[10] The direct peer-to-peer structure of cryptocurrency transactions eliminates intermediaries, insulating these operations from scrutiny and lowering the entry barrier for wider criminal participation.[10] The adoption of cryptocurrency broadens participation in BEC schemes and reshapes how illicit funds are laundered and repatriated. Are public sector organisations truly equipped to investigate the intersections of Black Axe and online fraud?

Implications for Counter-Fraud Measures:

The global reach and flexible organisational structure of Black Axe, particularly in their involvement with BEC scams, pose significant challenges to traditional counter-fraud measures. To address these complexities, public sector entities must implement a comprehensive, multi-faceted approach:

•**Stronger Regulatory Frameworks**: Governments must enforce stricter regulations around cryptocurrencies to curtail the laundering of illicit funds by cybercriminals.
•**Multi-Agency Collaboration**: International cooperation and intelligence-sharing among law enforcement, financial institutions, and public sector organisations are essential for tackling transnational cybercrime.
•**Investment in Technology**: Advanced cybersecurity tools are crucial for detecting and preventing BEC scams before they lead to substantial financial losses.
•**Education and Awareness**: Regular training for public and private sector employees can significantly reduce the success of phishing and social engineering techniques commonly used in BEC operations.

Will enhanced multi-agency collaboration suffice to combat transnational cybercrime, or are more radical reforms necessary?

References:

1. Lazarus S. Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the "Black Axe" confraternity. Deviant Behav 2024;1–25. https://doi.org/10.1080/01639625.2024.2352049
2. TESSIAN. 14 real-world examples of business email compromise (Updated 2022). Available from: https://www.tessian.com/blog/business-email-compromise-bec-examples/
3. CNN. A man who flaunted private jets and luxury cars on Instagram gets 11 years in prison for money laundering. Available from: https://edition.cnn.com/2022/11/08/us/instagram-star-ray-hushpuppi-sentenced-cec/index.html
4. Valimail. BEC scams cost companies $50 billion in losses. Available from: https://www.valimail.com/blog/bec-scams-cost-companies-50-billion-in-losses/
5. BBC. World's police in technological arms race with Nigerian mafia. Available from: https://www.bbc.co.uk/news/articles/c984w8jr1glo
6. Toronto Sun. Toronto romance scam linked to global fraud case. Available from: https://torontosun.com/2015/10/22/toronto-romance-scam-linked-to-global-fraud-case
7. Lazarus S, Button M. Tweets and reactions: Revealing the geographies of cybercrime perpetrators and the North-South divide. Cyberpsychol Behav Soc Netw 2022;25(8):504–511. https://doi.org/10.1089/cyber.2021.0332
8. Lazarus S, Olaigbe O, Adeduntan A, Dibiana ET, Okolorie GU. Cheques or dating scams? Online fraud themes in hip-hop songs across popular music apps. J Econ Crim 2023. https://doi.org/10.1016/j.jeconc.2023.100033
9. Lazarus S, Button M, Adogame A. Advantageous comparison: Using Twitter responses to understand similarities between cybercriminals ("Yahoo Boys") and politicians ("Yahoo men"). Heliyon 2022;8(11). https://doi.org/10.1016/j.heliyon.2022.e11142
10. Garba KH, Lazarus S, Button M. An assessment of convicted cryptocurrency fraudsters. Curr Issues Crim Justice 2024;1–17. https://doi.org/10.1080/10345329.2024.2403294