Научная статья
УДК 34:004:343.9:004.8
EDN: https://elibrary.ru/jvglrh
DOI: https://doi.org/10.21202/jdtl.2024.44

Социолого-криминологическое исследование проблем виктимизации: предварительный этап и новая область категоризации киберпреступности

Амину Мухаммад Аувал

Университет Джоса, Джос, Нигерия

Сулеман Лазарус ✉

Лондонская школа экономики и политических наук, Лондон, Великобритания
Университет Суррея, Гилфорд, Великобритания
Портсмутский университет, Портсмут, Великобритания

Ключевые слова

виктимизация,
виктимология,
жертва киберпреступления,
киберкриминология,
киберпреступность,
кибершпионаж,
онлайн-мошенничество,
правовая политика,
цифровая криминология,
цифровые технологии

Аннотация

Цель: выявление основных проблем виктимизации в результате роста киберпреступности в мире в целом и в нигерийском обществе в частности с позиций социологических подходов и с помощью трехчастной концепции киберпреступности (Tripartite Cybercrime Framework, TCF), состоящей из геополитических, психосоциальных и социально-экономических категорий киберпреступности.

Методы: основу методологии составили социологический метод исследования. Процесс сбора данных включал распространение опросника среди 896 участников из академической среды, в том числе студентов и сотрудников университета, и анализ ответов респондентов. Представленные данные анализировались с помощью описательной статистики, особое внимание при этом было уделено вопросам гендерного неравенства, социально-экономическим факторам, влиянию уровня образования на уязвимость к онлайн-мошенничеству и виктимизации в результате киберпреступлений через призму концепции идеальной жертвы и социально-экономического разрыва между Севером и Югом.

Результаты: в статье представлен анализ трехчастной концепции киберпреступности. На основе изучения данных, полученных в ходе анкетирования, установлено, что 65,20 % участников опроса когда-либо становились жертвами киберпреступников. Выявлен гендерный перекос среди жертв киберпреступлений в сторону мужчин (64,69 %).

✉ Корреспондирующий автор

Установлены закономерности в распределении киберпреступлений. Все киберпреступления против опрошенных лиц относились к категории социально-экономических, что подчеркивает распространенность киберпреступности и актуальность противодействия ей в нигерийском социуме. Особое внимание уделено вопросам гендерного неравенства, социально-экономическим факторам, влиянию уровня образования на уязвимость к киберпреступлениям. Проблема виктимизации рассмотрена с точки зрения концепции идеальной жертвы. **Результаты** исследования позволяют получить представление о распространенности и распределении конкретных видов киберпреступности социально-экономической категории среди исследуемой группы населения.

Научная новизна: в исследовании впервые используется подход трехчастной концепции киберпреступности (TCF) для изучения виктимизации в результате киберпреступлений в нигерийском обществе. Новизна представленного исследования обусловлена еще и тем, что сложившиеся на глобальном Севере концептуальные основы противодействия киберпреступности не вполне применимы в Нигерии.

Практическая значимость: полученные результаты демонстрируют необходимость применения тщательно выверенных гендерных, инклюзивных и контекстуальных подходов к разработке национальной правовой политики борьбы с киберпреступностью, могут быть положены в обоснование разрабатываемых правотворческих решений в области предупреждения и противодействия проявлениям киберпреступности, а также в основу правовых мер защиты жертв киберпреступлений.

Для цитирования

Аувал, А. М., Лазарус, С. (2024). Социолого-криминологическое исследование проблем виктимизации: предварительный этап и новая область категоризации киберпреступности. *Journal of Digital Technologies and Law*, *2*(4), 915–942. https://doi.org/10.21202/jdtl.2024.44

Содержание

Введение

Киберпреступность – глобальная проблема, однако пространственные характеристики влияют на поведение людей на местном уровне и могут быть выявлены или скрыты с помощью пространственных элементов (Hall & Yarwood, 2024; Lazarus & Button, 2022). Цель данной статьи – описать ситуацию с киберпреступностью и провести количественный анализ эмпирических данных. Киберпреступность представляет собой серьезную социальную проблему в Нигерии; в последние годы ее распространенность возросла (Ibrahim, 2016a; Idem & Olarinde, 2023). Жертвам киберпреступности в различных контекстах посвящены многие научные труды. Например, эту проблему изучали в Австралии (Cross, 2020; Drew & Webster, 2024), Китае (Wang, 2023), Португалии (Murça et al., 2024), Великобритании (Lazarus et al., 2022b), России (Timofeyev & Dremova, 2022). Жертвам киберпреступности в Нигерии посвящены лишь несколько исследований. В отличие от других стран, особенно таких как Австралия (Cross, 2020; Drew & Websters, 2024; Meikle & Cross, 2024) и Великобритания (Button et al., 2014, 2015, 2021), в Нигерии исследований жертв киберпреступности недостаточно.

Например, в работе Aborisade et al. (2024) были использованы интерпретативный феноменологический анализ и полуструктурированные видеоинтервью; опрошены десять жертв нигерийских брачных аферистов из шести разных стран. В исследовании Tade и Adeniyi (2017) проанализированы данные, полученные в ходе подробных интервью с жертвами мошенничества с банкоматами; было показано, что жертвы получили психологическую травму и часто обращались к друзьям, родителям и родственникам, чтобы справиться с последствиями. Однако ни в одном из этих исследований не использовались количественные методы для изучения демографических характеристик респондентов и их опыта борьбы

с киберпреступностью. Наша работа направлена на устранение этого пробела путем изучения демографических характеристик и опыта респондентов в отношении киберпреступности. В частности, была предпринята попытка изучить распространенность, характеристики и динамику сообщений о киберпреступлениях среди респондентов. Исследование призвано внести вклад в недостаточно разработанную тему виктимизации в результате киберпреступлений в нигерийском обществе, используя данные, собранные в ходе распределенного опроса.

1. Обзор литературы

1.1. Киберпреступность и киберкриминология

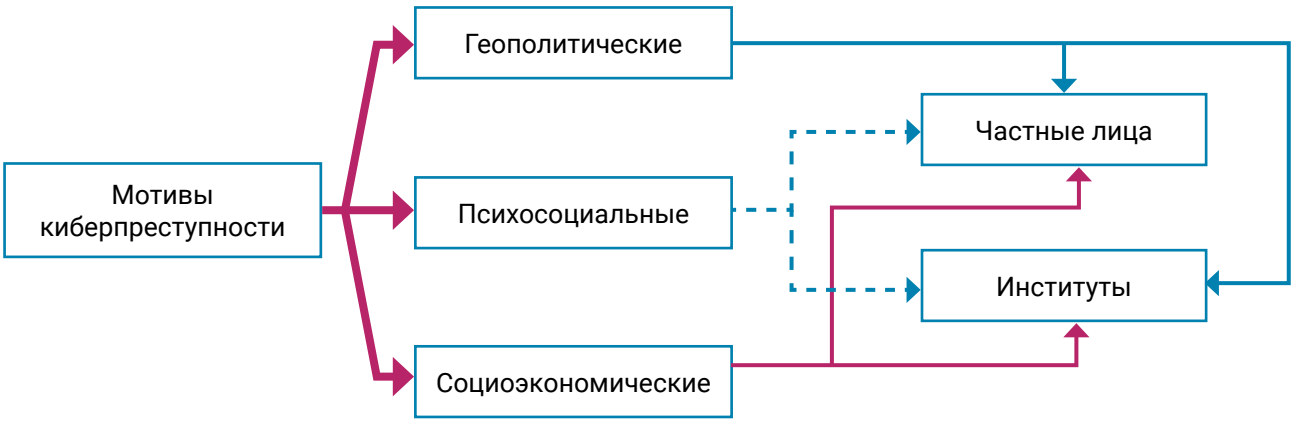
Идея о том, что разделение между физическим и цифровым мирами препятствует пониманию социальных сигналов в автономном режиме, которые также влияют на цифровую сферу, получила развитие в ряде работ (Jaishankar, 2007; Ibrahim, 2016a; Powell et al., 2018). Говоря о связи между офлайн- и онлайн-реальностью, исследователи использовали разные термины для выражения этой концепции. Например, McGerty (2000) писал, что «никто не живет только в киберпространстве», Jaishankar (2007, 2011, 2018) ввел понятие «киберкриминология», в то время как Powell с соавторами (2018) переименовали его в «цифровую криминологию». Эти различия в терминологии отражают споры в рамках научного дискурса по этой теме.

Понятие «киберпреступность» охватывает противоправную деятельность, осуществляемую с помощью Интернета и информационно-коммуникационных технологий (далее – ИКТ), включая «киберзависимые преступления» и «киберпреступления с использованием компьютерных технологий» (Button et al., 2023; Ibrahim, 2016a; Hall & Yarwood, 2024; Musotto & Wall, 2020). Они часто используются как синонимы для обозначения всех незаконных действий в Интернете, а органы безопасности, ученые и средства массовой информации часто объединяют различные цифровые правонарушения понятием «киберпреступность», игнорируя их уникальные признаки (Lazarus, 2019). Киберзависимые преступления совершаются даже без использования цифровых технологий или сетей, в то время как киберпреступления с использованием компьютерных технологий усугубляются за счет сетей. Мы фокусируемся на последней категории преступлений. Однако слияние таких категорий, как «киберпреступления с использованием компьютерных технологий»[1] и «киберпреступления, ориентированные на человека» (Gordon & Ford, 2006), затрудняет задачу разграничения между финансово мотивированными преступлениями, такими как «онлайн-мошенничество», и психологически мотивированными, такими как «порнография из мести» (Ibrahim, 2016a; Lazarus, 2019). В настоящей работе мы опираемся на подходы к киберпреступности, ориентированные на ситуацию в Нигерии, в частности, на концепцию Ibrahim (2016a). Тем самым мы стремимся внести свой вклад в дискуссию о виктимизации в результате онлайн-мошенничества и восполнить недостаточное внимание к идеям нигерийских ученых, как отмечено в работе Cross (2018a).

[1] McGuire, M., & Dowling, S. (2013, October). Cybercrime: a review of the evidence: Research Report 75. https://clck.ru/3F25c7

1.2. Трехчастная концепция киберпреступности (Tripartite Cybercrime Framework, TCF)

В эмпирической литературе (De Kimpe et al., 2020; Lazarus et al., 2022b) используется трехчастная концепция киберпреступности (Tripartite Cybercrime Framework, TCF). В ней проводится различие между киберпреступлениями, обусловленными психологией (психосоциальная киберпреступность), экономикой (социально-экономическая киберпреступность) и геополитикой. Это различие схематически показано на рисунке, основанном на оригинальной формулировке Ibrahim (2016a). В работе Ibrahim (2016a) разъясняется, что, хотя в нигерийском контексте киберпреступления обусловлены в первую очередь финансами, не все киберпреступления с использованием компьютерных технологий таковы, например, порнография из мести. Основываясь на этой классификации, мы выделяем уникальные характеристики киберпреступлений в Нигерии как особой подгруппы преступлений. Киберпреступность действительно является глобальной проблемой. Однако она также обладает пространственными характеристиками, влияющими на поведение людей в определенных регионах и проявляющимися в пространственных элементах, которые могут быть скрыты или выявлены (Hall & Yawood, 2024; Lazarus & Button, 2022).



Трехчастная концепция киберпреступности (Tripartite Cybercrime Framework, TCF)

1.2.1. Геополитическая категория киберпреступности

Геополитическая киберпреступность включает в себя киберпреступления, совершаемые по политическим мотивам, часто с участием государственных структур, негосударственных активистов или их представителей (Ibrahim, 2016a; Lazarus, 2019). Эти действия могут включать кибершпионаж или атаки на критически важную инфраструктуру. Однако киберпреступность, исходящая из Нигерии, редко попадает в эту категорию, в отличие от других стран, таких как Соединенные Штаты и Китай (Ibrahim, 2016a). Например, спонсируемые государством хакерские группы могут быть нацелены на иностранные правительственные учреждения с целью сбора разведданных для получения политических преимуществ в дипломатических переговорах или военных стратегиях (Akoto, 2021; Makridis et al., 2024). Основная мотивация этой категории киберпреступности носит политический характер, что соответствует геополитической категории в модели TCF (Ibrahim, 2016a).

1.2.2. Психосоциальная категория киберпреступности

Психосоциальная киберпреступность включает в себя преступления в сфере цифровых технологий, которые в первую очередь обусловлены психологическими мотивами и направлены на причинение страданий, мучений или вреда отдельным лицам (Ibrahim, 2016a; Lazarus, 2019). Денежная выгода в таких случаях не является основной целью. Примерами могут служить киберпреследование, киберзапугивание и онлайн-насилие, нацеленные на жертв в социальных сетях с целью нанести им психологический вред и подорвать их репутацию. Преступники получают удовлетворение от причинения страданий, что подчеркивает психосоциальный характер этих преступлений (Ibrahim, 2016a; Lazarus, 2019). Хотя преступники, занимающиеся порнографией из мести, часто обвиняют и унижают жертв, в случае мошенничества это не является основным мотивом, которым в этом случае являются деньги.

1.2.3. Социально-экономическая категория киберпреступности

Социально-экономическая киберпреступность связана с получением финансовой выгоды путем обмана с помощью компьютерных или интернет-технологий. Сюда относятся такие незаконные действия, как онлайн-мошенничество, брачные аферы, кража авторских прав и незаконное скачивание цифрового контента (Ibrahim, 2016a). Нигерия особенно уязвима к киберпреступлениям, относящимся к этой категории, включая подчинение, выдачу себя за законного пользователя, манипулирование, подделку документов, подлог, введение в заблуждение. Среди известных примеров – брачные аферы онлайн (Drew & Webster, 2024; Lazarus et al., 2023) и мошенническая схема «забой свиней» (Wang, 2023; Whittaker et al., 2024). Эти преступные схемы в первую очередь мотивированы финансовой выгодой.

Однако геополитические, психосоциальные и социально-экономические категории не определены жестко, и может иметь место сочетание нескольких мотивов. Например, если хактивисты [хакер-активист. – Прим. переводчика] публикуют украденную личную информацию в политических целях, то это может иметь психологические и геополитические последствия. Тем не менее TCF служит полезным инструментом для классификации отличительных особенностей различных киберпреступлений в Нигерии и за ее пределами. В Нигерии отсутствует статистика по другим видам киберпреступлений, например, кибершпионажу, киберпреследованиям и порнографии из мести, которые более распространены в таких странах, как Бельгия, Канада и Великобритания (Ibrahim, 2016a). Таким образом, концептуальные основы борьбы с киберпреступностью на глобальном Севере не вполне применимы в Нигерии, представляющей страны Африки к югу от Сахары (Ibrahim, 2016a). Стоит отметить, что ситуация с киберпреступностью в Нигерии сложна.

1.3. Проблемы и вызовы киберпреступности в Нигерии

Материалы недавних конференций проливают свет на различные аспекты судебного преследования за киберпреступления, регулирования и их влияния на ситуацию в Нигерии. Так, Idem с соавторами (2023a) выявили ключевые проблемы, препятствующие судебному преследованию киберпреступников в Нигерии, среди которых отсутствие четкого законодательства, неэффективное правоприменение,

судебные проволочки и ограниченные возможности криминалистического анализа. Основываясь на этом анализе, Idem и соавторы (2023b) подчеркивают настоятельную необходимость реформы органов по регулированию киберпреступности, чтобы изменить статус Нигерии как одной из трех стран с наибольшим ростом киберпреступности. Аналогичным образом, Idem (2023) предполагает, что принятый в Нигерии Закон о киберпреступности сыграл значительную роль в регулировании и сдерживании различных форм киберпреступности, защите и продвижении онлайн-бизнеса. Эти три взаимосвязанных исследования в совокупности освещают многогранные проблемы, связанные с киберпреступностью в Нигерии, и подчеркивают важность законодательных, нормативных и социально-экономических мер для их решения.

Далее, в работах Ojolo и Adewumi (2020) и Lazarus с соавторами (2023) освещается нормализация обстановки с киберпреступностью в нигерийском обществе, хотя выделены такие важные факторы ее распространения, как экономическая нестабильность, коррупция и влияние сверстников. В свою очередь, Lazarus с соавторами (2022a) проводят параллели между интернет-мошенниками (Yahoo Boys) и коррумпированными политиками (Yahoo Men) в Нигерии. Аналогичным образом, Olaiya с соавторами (2020), Monsurat (2020) и Adeduntan (2022) подчеркивают влияние политической коррупции, давления со стороны сверстников, экономических трудностей и неадекватных систем социальной поддержки. Кроме того, Ojolo и Singh (2023) и Aransiola и Asindemade (2011) раскрывают прибыльный характер этой деятельности и причастность коррумпированных сотрудников правоохранительных органов и отмечают, что финансовые стимулы пересекаются с институциональной уязвимостью, способствуя незаконным онлайн-практикам. В совокупности вышеприведенные исследования показывают, что киберпреступность – это сложное явление, коренящееся в социально-экономическом неравенстве, недостатках институциональной системы и культурных влияниях. При этом существует четкая закономерность, согласно которой в последние годы число случаев киберпреступности увеличилось.

1.4. Рост экономической киберпреступности в Нигерии

Рост экономической киберпреступности в Нигерии вызывает обеспокоенность у различных заинтересованных сторон. Idem и Olarinde (2023) освещают негативное влияние киберпреступности на развитие молодежи, экономику и управление в Нигерии. В качестве основных факторов вовлечения молодежи в киберпреступную деятельность они определяют безработицу, бедность, коррупцию и неэффективное управление, предлагая рекомендации по борьбе с этими проблемами. Согласно анализу отчетов о киберпреступлениях и инцидентах в области кибербезопасности, опубликованных Комиссией по экономическим и финансовым преступлениям (Economic and Financial Crimes Commission, EFCC)[2] за период с 2019 по 2022 г., число случаев онлайн-мошенничества резко возросло. Обобщим эту информацию, дающую представление о распространенности киберпреступности в нигерийском обществе, когда за четырехлетний период наблюдений резко увеличилось число вынесенных приговоров.

[2] EFCC, 2022: https://goo.su/TJjHS

Так, в период с 2019 по 2022 г. отмечено существенное увеличение числа сообщений о киберпреступлениях. В 2019 г. 877 человек сообщили об инцидентах, связанных с киберпреступностью; в 2020 г. это число увеличилось до 1890, т. е. на 115,5 %. В 2021 г. число зарегистрированных инцидентов увеличилось до 2400, что отражает ошеломляющий рост на 173,7 % по сравнению с базовым показателем 2019 г. Прогнозы на 2022 г. указывали на продолжающуюся тенденцию к росту: зарегистрировано 2900 инцидентов, что на 230,7 % больше по сравнению с первоначальными показателями 2019 г. Эти статистические данные свидетельствуют об экспоненциальном росте онлайн-мошенничества и подчеркивают необходимость научного исследования моделей виктимизации в стране. Наш анализ показывает заметный всплеск активности в сфере киберпреступности, что подтверждает растущее число осужденных за киберпреступления, о которых сообщает EFCC. Статданные доказывают значительный рост киберпреступности в Нигерии за указанный период, что говорит об активизации деятельности киберпреступных организаций, в первую очередь Yahoo Boys (Aborisade, 2023; Lazarus & Okolorie, 2019; Ogunleye et al., 2019; Ojedokun & Eraye, 2012).

1.5. Исследования, ориентированные на жертв преступности

Действия Yahoo Boys имеют глобальные последствия, что привело к увеличению числа исследований, затрагивающих проблему жертв онлайн-мошенничества. На тему виктимизации было проведено множество исследований, но большинство из них были посвящены западным обществам и азиатским странам, таким как Китай. В ряде исследований рассматривались такие африканские страны, как Нигерия, но они относительно редки. Например, исследования Button с соавторами (2014), Meikle & Cross (2024), Drew & Websters (2024), Cross (2020, 2018b), Whitty (2019) в основном фокусируются на жертвах из западных обществ и азиатских стран, таких как Китай (Tao, 2022; Wang, 2023; Wang & Topalli, 2024). Лишь немногие исследователи, такие как Aborisade с соавторами (2024), изучали виктимизацию в африканских странах, в частности, в Нигерии. Этот дисбаланс может быть вызван тем, что западные СМИ освещают исключительно жертв из западных стран, а также приоритетами в распределении финансирования исследований. Подобные тенденции закрепляют неравенство и непреднамеренно маргинализируют жертв из Нигерии. Наше исследование направлено на устранение этого неравенства; мы подчеркиваем, что пагубное влияние Yahoo Boys распространяется за пределы страны и выходит на глобальную арену. Освещая опыт жертв преступлений в таких африканских странах, как Нигерия, мы стремимся оспорить распространенный западноцентричный подход и подчеркнуть универсальность проблемы. Инклюзивный подход способствует более глубокому пониманию онлайн-мошенничества и его воздействия на жертв во всем мире.

1.6. Киберпреступники в нигерийском обществе (Yahoo Boys)

В ходе ряда качественных исследований были изучены действия нигерийских киберпреступников как внутри страны (Aransiola & Asindemade, 2011; Lazarus & Okolorie, 2019; Ogunleye et al., 2019; Ojedokun & Eraye, 2012), так и за ее пределами (Lazarus, 2024). Это позволило получить представление о различных аспектах деятельности этих преступников. Приведенная выше эмпирическая литература

неизменно указывает на то, что основными виновниками киберпреступлений являются лица мужского пола. Именно они в основном координируют социально-экономические цифровые преступления в Интернете, как показано на рисунке. Напротив, согласно свидетельствам, девушки-студентки, совершающие онлайн-мошенничества, преимущественно занимают подчиненные позиции при руководителях-мужчинах (Ogunleye et al., 2019). Приведенные выше результаты относятся к нигерийскому обществу, подчеркивая, что мужчины являются основными виновниками этих киберпреступных действий. Однако лишь в ограниченном числе исследований, включая работу Aborisade с соавторами (2024), был изучен опыт жертв киберпреступности в Нигерии.

1.7. Сходство и различия с предыдущими исследованиями

В нигерийском контексте многие исследования с использованием различных источников данных привели к сходным результатам. К ним относятся интервью с рядовыми сотрудниками правоохранительных органов (Lazarus & Okolorie, 2019), анализ мошеннических электронных писем (Genc et al., 2021; Rich, 2018), изучение текстов песен (Adeduntan, 2022; Lazarus et al., 2023), интервью с родителями (Aborisade, 2023; Ibrahim, 2016b), интервью с онлайн-мошенниками (Aransiola & Asindemade, 2011; Lazarus, 2024; Ojedokun & Eraye, 2012; Ogunleye et al., 2019), изучение твитов (Lazarus & Button, 2022). Последовательные и совпадающие результаты этих работ существенно повышают достоверность эмпирических исследований в целом, тем самым подтверждая фундаментальное понимание характеристик онлайн-преступников и категории киберпреступлений, которые они совершают. Более того, работы, не основанные на эмпирических данных, подтверждают выводы эмпирических исследований (Idem et al., 2023a, 2023b). Таким образом, выявленные признаки подкреплены данными, полученными с помощью различных методологий исследования. В Нигерии было проведено лишь ограниченное число исследований, посвященных жертвам киберпреступности, в частности, Aborisade et al. (2024), Mba et al. (2017), Tade и Adeniyi (2017).

1.8. Новизна данной работы

Настоящее исследование отличается от предыдущих в нескольких отношениях. Ранее при изучении жертв киберпреступлений в Нигерии (Aborisade et al., 2024; Mba et al., 2017; Tade & Adeniyi, 2017) не использовалось анкетирование. Предыдущие подходы, такие как в работе Aborisade с соавторами (2024) и Tade и Adeniyi (2017), основывались на качественных методах. В работе Mba с соавторами (2017) использовались данные форума сайта www.topix.com и поисковые системы в Интернете для выявления активных мошеннических и подобных онлайн-сообщений. В эмпирических исследованиях, в частности, бельгийских ученых De Kimpe с соавторами (2020), отправной точкой служила трехчастная концепция киберпреступности (TCF); однако эта концепция никогда не использовалась в явном виде, за исключением работы Lazarus с соавторами (2022b), в которой объединяются подходы TCF и феминистской эпистемологии преступности. В то же время Lazarus с соавторами (2022b) исследовали восприятие киберпреступлений в соответствии с категориями TCF в Великобритании, тогда как наше исследование направлено на изучение виктимизации в результате киберпреступлений в Нигерии через призму классификаций TCF. В качестве основы для нашего исследования мы используем «Социально-экономическую теорию киберпреступности в Нигерии», предложенную Ibrahim (2016a).

2. Методы и материалы

Для сбора данных мы использовали метод распределенного опроса различных групп студентов, сотрудников и работников из разных секторов экономики. Анкета разработана на основе концепции Ibrahim (2016a), которая подразделяет киберпреступность на социально-экономическую, геополитическую и психосоциальную категории, что позволяет выявить нюансы и особенности типов киберпреступности в Нигерии. Опрос проводился среди добровольных участников из разных демографических групп, которые могли тем самым лучше понять проблему киберпреступности. Хотя ответы участников были анонимными и конфиденциальными, для обеспечения соблюдения принципов научного исследования мы получили одобрение Совета по этике одного из университетов в Нигерии. Анкета была тщательно разработана и распространена через имеющиеся платформы для проведения опросов, что обеспечило эффективность и широкий охват исследования. Участники предоставили информированное согласие перед началом работы; были приняты строгие меры для обеспечения их анонимности и конфиденциальности на протяжении всего процесса сбора данных.

2.1. Анализ данных

Для определения географических кластеров и секторов, наиболее подверженных киберпреступности, мы провели анализ данных соседних стран. В сочетании с простыми статистическими методами и расширенной пространственной статистикой анализ данных позволил получить важную информацию о распространенности и характеристиках киберпреступности в исследуемой популяции. Кроме того, мы провели статистический анализ для выявления тенденций и закономерностей в частоте совершения киберпреступлений за определенный период. Описательные статистические данные, такие как средние значения и медианы, были рассчитаны с использованием электронных таблиц Excel, получены соответствующие количественные и процентные показатели. Хотя этот метод имеет свои ограничения, он обоснован с помощью следующих методов:

1. Исследовательский анализ. Описательная статистика служит ценным инструментом для проведения исследовательского анализа, позволяя получить первоначальное представление о данных путем обобщения ключевых характеристик, таких как центральная тенденция и изменчивость. Поскольку это предварительный этап исследования, такой подход позволяет выявить основные закономерности, связанные с киберпреступностью, не предполагая лежащих в их основе взаимосвязей, что важно, учитывая сложную социокультурную структуру нигерийского общества.

2. Представление данных. Описательная статистика имеет решающее значение для представления основных выводов в ясной и сжатой форме, что делает их доступными для широкой аудитории, включая студентов различных специальностей. Учитывая, что исследование фокусируется на опыте столкновения с киберпреступностью среди студентов и сотрудников университетов в Нигерии, описательная статистика позволяет напрямую донести важные выводы о распространенности и характеристиках киберпреступности до представителей этой группы населения.

3. Простые структуры данных. Инструментарий, использованный в исследовании, имеет относительно простую структуру с небольшим количеством переменных и прямыми взаимосвязями. Таким образом, описательная статистика хорошо подходит для решения поставленных задач и достижения целей данного

предварительного исследования. По итогам работы авторы пришли к выводу, что в более сложных аналитических методах нет необходимости, так как они лишь привели бы к излишней усложненности. Описательная статистика является эффективным способом анализа и обобщения данных, предоставляя ценную информацию об опыте виктимизации в результате киберпреступлений среди исследуемой группы населения.

3. Результаты

В данном разделе представлены результаты количественного анализа 896 ответов респондентов с указанием частот и процентных соотношений по каждой категории преступлений. Результаты показаны в таблице. Почти все участники (99,78 %) дали свое информированное согласие, что свидетельствует о высоком уровне готовности участвовать в исследовании. Лишь небольшая часть (0,76 %) предпочла не давать согласия, что говорит о том, что большинство участников были готовы к участию в опросе.

Краткое изложение результатов

Вопрос	Ответ	Кол-во	Процент
Получено информированное согласие	Да	896	99,78
	Нет	7	0,76
Распределение респондентов по полу	Мужской	584	64,69
	Женский	312	34,52
Уровень образования	Магистрант	522	57,80
	Аспирант	21	2,36
	Преподаватель и руководство	12	1,35
Становились ли жертвами киберпреступления	Да	588	65,20
	Нет	301	33,40
Пол жертвы киберпреступления	Мужской	303	51,53
	Женский	285	48,47
Тип киберпреступления, с которым сталкивались	Мошенничество с онлайн-банком/платежами/картами	554	61,45
	Кража личности	67	7,43
	Другое	295	32,68
Сообщали ли о киберпреступлении	Да	322	35,74
	Нет	577	63,94
Были ли возвращены украденные деньги/предприняты надлежащие меры	Да	54	5,99
	Нет	835	92,61

3.1. Гендерный аспект

Результаты исследования проливают свет на гендерную динамику виктимизации в результате киберпреступлений, выявляя заметное различие в опыте мужчин и женщин. Анализ данных показывает, что среди лиц, пострадавших от киберпреступности, 303 мужчины (51,53 %) и 285 женщин (48,47 %) сообщили о неблагоприятных последствиях. Это неравенство еще больше подчеркивается общим распределением жертв киберпреступлений: 64,69 % мужчин и 34,52 % женщин. Эти цифры свидетельствуют о гендерном характере виктимизации в результате киберпреступлений:

более высокая доля мужчин сталкивается с негативными последствиями по сравнению с женщинами. Полученные данные также подчеркивают необходимость применения гендерно ориентированных подходов к борьбе с киберпреступностью и принятия мер по смягчению ее последствий как для мужчин, так и для женщин. Кроме того, относительно сбалансированное распределение жертв среди мужчин и женщин подчеркивает важность учета гендерной динамики при понимании явлений киберпреступности и реагировании на них.

3.2. Уровень образования

Участники имели различный уровень образования. 37,80 % из них были студентами бакалавриата, 57,80 % – магистрантами, 2,36 % – аспирантами и 1,35 % – преподавателями и административными сотрудниками вуза. Такое разнообразие уровней образования усиливает неоднородность выборки и делает выводы более обобщающими.

3.3. Подтвержденный негативный опыт в сфере киберпреступности

Значительная часть участников (65,20 %) сообщили, что сталкивались с негативными инцидентами, связанными с киберпреступностью, что подчеркивает ее повсеместное воздействие на исследуемую группу населения. Однако 33,40 % респондентов указали, что они не сталкивались с какими-либо инцидентами, связанными с киберпреступностью, что указывает на наличие подгруппы лиц, не затронутых этим видом преступлений.

3.4. Типы киберпреступлений

Исследование выявило четкие закономерности в распределении киберпреступлений. Мошенничество с использованием электронных банковских услуг/платежных карт было наиболее распространенным видом мошенничества, на долю которого приходилось 61,45 % зарегистрированных случаев. На кражу личных данных приходилось 7,43 % инцидентов, в то время как на другие формы кражи в совокупности – 32,68 % случаев, таких как мошенничество с трудоустройством в Интернете. Эти данные позволяют получить представление о распространенности и распределении конкретных видов киберпреступности социально-экономической категории среди исследуемой группы населения.

3.5. Сообщения об инцидентах

Исследование показало, что 35,74 % участников сообщили об инцидентах, связанных с киберпреступностью, в соответствующие органы или организации, что свидетельствует об умеренном использовании соответствующих механизмов. Напротив, большинство (63,94 %) не сообщали о каких-либо инцидентах, что свидетельствует о возможном занижении отчетности и областях, требующих улучшения этой сферы правоохранительной практики.

3.6. Возврат украденных денег/Принятие соответствующих мер

Среди участников, сообщивших об инцидентах, связанных с киберпреступностью, лишь меньшинство (5,99 %) указали, что украденные средства были возвращены или в ответ были приняты соответствующие меры. И наоборот, подавляющее

большинство (92,61 %) сообщили об отсутствии мер по исправлению положения, что указывает на трудности в достижении реституции или разрешении проблемы после того, как они стали жертвами киберпреступлений. Эти результаты дают ценную информацию о распространенности киберпреступности, ее характеристиках и динамике сообщений среди участников, однако необходимы дальнейшие исследования для сравнения с имеющейся эмпирической литературой и выявления возможных последствий для политики, практики и будущих исследований.

4. Обсуждение

В данном разделе мы, опираясь на информацию, полученную с помощью метода распределенного опроса, попытаемся изучить проблему виктимизации в результате киберпреступлений в различных демографических группах. Мы рассмотрим четыре основные темы: (1) различия в опыте столкновения с киберпреступностью по гендерному признаку; (2) ключевая роль социально-экономических факторов в борьбе с киберпреступностью в Нигерии; (3) взаимосвязь между уровнем образования и уязвимостью к онлайн-мошенничеству и (4) исследование виктимизации в результате киберпреступности через призму социально-экономического разрыва между Севером и Югом.

4.1. Гендерный аспект виктимизации в результате онлайн-мошенничества

Проведенный анализ гендерных различий в виктимизации в результате киберпреступлений (таблица, п. 3.4 статьи) частично согласуется с результатами предыдущих исследований, но и расходится с ними. Например, согласно работе Lazarus с соавторами (2022b), женщины склонны воспринимать психосоциальные киберпреступления, такие как порнография из мести, как более тяжелые, чем мужчины; однако в отношении социально-экономических киберпреступлений, таких как онлайн-мошенничество с кредитными картами, заметных гендерных различий не наблюдается. Примечательно, что в отличие от вышеприведенных авторов наше исследование не изучает напрямую восприятие киберпреступности, но показывает гендерные различия в социально-экономической виктимизации в результате киберпреступности, что вносит свой вклад в научную дискуссию. Более того, многочисленные исследования (Näsi et al., 2023) позволили изучить сложную динамику виктимизации в результате киберпреступлений, пролив свет на различные влияющие на нее факторы. Исследование Kadoya с соавторами, проведенное в 2021 г. в Японии, указывает на пол и семейное положение в качестве потенциальных факторов, определяющих виктимизацию; другими словами, мужчины и состоящие в браке люди более подвержены мошенничеству с банковскими счетами. Аналогичным образом, исследование Whitty (2019), проведенное в Великобритании, подчеркивает гендерные различия в киберпреступности, особенно очевидные в случае брачных аферистов, где женщины подвергаются непропорциональной виктимизации. Хотя в нашем исследовании конкретно не задавались вопросы о семейном положении или брачных аферах, наши выводы перекликаются с выводами Kadoya с соавторами (2021) и Whitty (2019), подтверждающими важность гендерного фактора в виктимизации в результате киберпреступности.

Вариативность гендерного неравенства в различных контекстах дополнительно подтверждается исследованиями, проведенными в Финляндии (Näsi et al., 2023) и Нидерландах (Weijer et al., 2020). Первое не выявило статистически значимых

гендерных различий, однако голландское исследование показало, что женщины чаще сообщают в полицию о традиционных преступлениях, в то время как мужчины проявляют большую активность в сообщениях о киберпреступлениях (Näsi et al., 2023; Weijer et al., 2020). Следовательно, можно с уверенностью утверждать, что гендерные различия, выявленные в нашем исследовании, могут быть частично объяснены различиями в поведении при сообщении о преступлениях. Это подчеркивает неоднозначность данных о кибервиктимизации: о киберпреступлениях часто сообщают не в полицию, а в другие организации. Кроме того, гендерные различия существенно влияют на подверженность онлайн-мошенничеству, а такие психологические особенности, как склонность к риску и низкий уровень самоконтроля, еще больше повышают уязвимость (Norris et al., 2019). Хотя мы не изучали психологические особенности и их связь с виктимизацией при онлайн-мошенничестве, наши результаты свидетельствуют о том, что гендерные различия существенно влияют на подверженность онлайн-мошенничеству. Несмотря на эти гендерные нюансы, сам по себе гендер играет лишь второстепенную роль в прогнозировании кибервиктимизации, в то время как значительное влияние оказывают другие факторы, такие как мотивация мошенников и уязвимость цели.

4.2. Роль киберпреступности в социально-экономической динамике

Наше исследование выявило четкие тенденции в области киберпреступлений, в частности, выделив мошенничество с использованием электронных банковских услуг/платежных карт как наиболее распространенный вид преступлений, на который приходится 61,45 % всех зарегистрированных случаев (табл). На кражу личных данных приходилось 7,43 % инцидентов, в то время как на различные другие виды мошенничества, включая мошенничество с поиском работы в Интернете и фишинговые схемы, в совокупности приходилось 32,68 % случаев, и все они подпадали под социально-экономическую категорию киберпреступности (табл). Это подтверждает тот факт, что киберпреступность имеет пространственные характеристики, поскольку она распространяется, проявляется и влияет на поведение людей по-разному в различных регионах, а также может быть скрыта или выявлена с помощью пространственных элементов (Hall & Yawood, 2024; Lazarus & Button, 2022). Трехчастная концепция киберпреступности (TCF) подразделяет киберпреступления на три основных категории согласно мотивации: социально-экономическую, психологическую и геополитическую, подчеркивая различие между социально-экономическими и психосоциальными киберпреступлениями (Ibrahim, 2016a; Lazarus, 2019; Lazarus et al., 2022b).

В отличие от таких стран, как Канада, Россия, Китай и Великобритания, в Нигерии отсутствует существенная статистика по другим категориям киберпреступлений, в частности по геополитическим, таким как кибершпионаж, и психосоциальным, таким как порнография из мести (Ibrahim, 2016a). Геополитический и социокультурный контексты разных стран существенно влияют на их поведение в киберпространстве. Например, порнография из мести распространена в таких западных странах, как Португалия (Murça et al., 2024), Великобритания, Канада и др. (Harper et al., 2023), в то время как в Нигерии она не так заметна. Кроме того, в отличие от Нигерии, такие страны, как Соединенные Штаты, Россия, Китай и Великобритания, сталкиваются со значительными проблемами, связанными с кибершпионажем, спонсируемым государством (Akoto, 2021, 2024; Markridis et al., 2024). Эти социальные и контекстуальные нюансы бросают вызов представлениям о киберпространстве и физическом

пространстве как об отдельных сущностях с четкими границами, что подчеркивал Jaishankar (2007, 2011, 2018). В результате концептуальные рамки, обычно используемые в отношении «глобального Севера», могут быть не совсем применимы в Нигерии, представляющей Африку к югу от Сахары (Ibrahim, 2016a). Сложность ситуации с киберпреступностью в Нигерии очевидна. Хотя данные нашего опроса были получены из одного учреждения, результаты позволяют судить о распространенности и распределении видов киберпреступности в рамках категории социально-экономических преступлений.

Хотя в Нигерии нет существенной статистики по определенным категориям киберпреступлений, это не обязательно означает, что психосоциальные киберпреступления, такие как киберпреследование и киберзапугивание, отсутствуют или незначительны. Одно из возможных объяснений заключается в том, что социокультурная структура нигерийского общества определяет приоритетность социально-экономических видов киберпреступлений, таких как онлайн-мошенничество. Этот акцент проявляется в том, что EFCC, один из высших правоохранительных органов Нигерии, уделяет особое внимание финансовым преступлениям. Кроме того, отсутствие статистики может быть вызвано другими факторами, такими как ограниченные ресурсы или недостаточность инфраструктуры для выявления подобных киберпреступлений и сообщения о них. Также, хотя социокультурный и геополитический контексты влияют на поведение в киберпространстве, важно признать, что геополитические виды киберпреступлений часто не затрагивают обычных граждан, таких как студенты и преподаватели, которых мы изучали в данной работе. В результате наше исследование не охватывало геополитические аспекты, что может привести к неточностям в наших выводах.

4.3. Уровень образования жертв онлайн-мошенничества

Один из важных выводов, сделанных в ходе нашего исследования, касается уровня образования участников. Хотя более 99 % из них имели высшее образование или находились в процессе его получения, уровни образования значительно различались. В частности, среди участников 37,80 % были студентами бакалавриата, 57,80 % – магистрантами, 2,36 % – аспирантами и 1,35 % были преподавателями и административными сотрудниками вуза (п. 3.2 статьи). Несмотря на такое разнообразие в уровне образования, более 65 % всех участников сообщили, что стали жертвами киберпреступлений, и этот вывод частично согласуется с предыдущими исследованиями, но и расходится с ними.

Существующие исследования показывают, что на вероятность стать жертвой онлайн-мошенничества влияют несколько факторов, среди которых значительную роль играет уровень образования. Исследования показали, что лица с более низким уровнем образования более подвержены мошенничеству в потребительской сфере (Whitty, 2018). Однако исследования также свидетельствуют о наличии сложной взаимосвязи между уровнем образования и жертвами мошенничества. Например, люди, находящиеся на самом низком уровне образования, не имеющие законченного среднего или высшего образования, с меньшей вероятностью становятся жертвами мошенничества (Schoepfer & Piquero, 2009), что указывает на U-образную закономерность в этой взаимосвязи.

Более того, люди, получившие высшее образование и проводящие больше времени в Интернете, подвергаются большему риску стать мишенью мошенников (Paek & Nalla, 2015). Эта связь подчеркивает влияние повседневной онлайн-активности на риск виктимизации, а также роль онлайн-взаимодействий в повышении уязвимости к киберпреступности. Кроме того, пожилые люди, которые, как правило, имеют более высокий уровень образования, считаются особенно уязвимыми для кибермошенничества (Whitty, 2019). Эта демографическая группа часто проявляет такие черты, как высокая импульсивность, склонность к рискованному поведению в Интернете и тенденцию к зависимостям, что повышает их восприимчивость к онлайн-мошенничеству.

4.4. Виктимизация в результате киберпреступлений, концепция идеальной жертвы и разрыв между Севером и Югом

Результаты нашего исследования подчеркивают повсеместное влияние киберпреступности в Нигерии, при этом заметное большинство участников (65,20 %) сообщили о личном опыте виктимизации (Aborisade et al., 2024). Это говорит о широкомасштабном характере киберпреступности и ее существенном влиянии на исследуемую группу населения. И наоборот, 33,40 % респондентов указали, что они не сталкивались с инцидентами, связанными с киберпреступностью, что указывает на то, что в Нигерии есть группа лиц, не затронутых этой преступной деятельностью. Это противоречие заставляет задуматься о теории виктимизации и различиях между глобальным Севером и Западной Африкой (Нигерией), что редко рассматривается в литературе по онлайн-мошенничеству.

Группа Yahoo Boys, зародившаяся в Нигерии, но осуществляющая деятельность по всему миру, привлекла повышенное внимание к жертвам онлайн-мошенничества. Однако существующие исследования в основном сосредоточены на жертвах из западных обществ (Button et al., 2014, 2015; Cross, 2020; Drew & Webster, 2024) и на некоторых незападных контекстах, таких как Китай (Tao, 2022; Wang, 2023); при этом странам Западной Африки, таким как Нигерия, посвящено ограниченное количество исследований (Aborisade et al., 2024). Вполне вероятно, что неравномерное распределение исследовательского интереса к определенным вопросам объясняется тенденцией западных СМИ уделять особое внимание громким инцидентам с жертвами из западных стран. Кроме того, финансирование научных исследований часто ориентировано в первую очередь на Запад, что приводит к недостатку внимания и ресурсов для других регионов, включая западноафриканские страны, такие как Нигерия (Mosbah-Natanson & Gingras, 2014). Эти предубеждения закрепляют предвзятость и непреднамеренно маргинализируют жертв из незападных стран, тем самым подчеркивая концепцию «идеальных жертв», когда некоторые жертвы могут считаться более «идеальными», чем другие. Жертвы онлайн-мошенничества в западных обществах, таких как Соединенные Штаты, Великобритания и Австралия, имеют такое же значение, как и в Нигерии.

Опираясь на основополагающую работу Christie (1986), в которой описываются черты идеальной жертвы, наше исследование изучало динамику виктимизации в результате онлайн-мошенничества в контексте Нигерии. Christie (1986) утверждает, что идеальные жертвы воспринимаются как воплощения определенных черт, соответствующих общественным нормам невиновности, уязвимости и отсутствия вины,

что вызывает положительную реакцию общества. Такой общественный резонанс потенциально может предотвратить преступления или способствовать привлечению преступников к ответственности. Другие ученые использовали эту концепцию для изучения аспектов киберпреступности (Hock & Button, 2023; Loyens & Paraciani, 2023). Используя эту концепцию, мы рассматриваем не только динамику мошеннических преступлений, нацеленных на нигерийцев, но и реакцию мирового сообщества на преступления, жертвами которых становятся нигерийцы, включая выделение средств на исследования в этой области. Мы утверждаем, что соотношение сил между глобальными Севером и Югом, наряду со структурой мировой экономики, формирует отношение к жертвам. При этом жертвы из стран Запада воспринимаются как более заслуживающие статуса «идеальной жертвы», чем нигерийцы, что влияет как на региональные, так и на глобальные меры реагирования на преступления, совершаемые против нигерийцев. С учетом значительного роста числа жертв онлайн-мошенничества в Нигерии, например, в период с 2019 по 2022 г. этот вопрос вызывает глубокую озабоченность.

Однако стоит отметить, что динамика сил и экономические структуры, которые формируют отношение к жертвам, сложны и многогранны, и их не следует чрезмерно упрощать или сводить к одному фактору. Кроме того, региональные власти и правительство Нигерии несут главную ответственность за своих граждан и не должны перекладывать на внешние органы и международные сообщества (например, на западные страны) свои обязанности по оказанию поддержки жертвам онлайн-мошенничества в нигерийском обществе. Наконец, хотя ситуация с онлайн-мошенничеством действительно вызывает серьезную озабоченность в Нигерии, это явление не уникально и встречается также во многих других частях мира.

Заключение

Наше исследование с участием 896 человек позволило получить представление о виктимизации в результате киберпреступлений. Особое внимание было уделено вопросам гендерного неравенства, социально-экономическим факторам, влиянию уровня образования на уязвимость к онлайн-мошенничеству и виктимизации в результате киберпреступлений через призму концепции идеальной жертвы и социально-экономического разрыва между Севером и Югом. Наш анализ выявил гендерные различия в опыте виктимизации в результате киберпреступлений: более высокая доля мужчин сталкивается с негативными последствиями киберпреступлений, что согласуется с предыдущими исследованиями (Kadoya et al., 2021). Работа предлагает новый взгляд на этот дискурс, подчеркнув вариативность гендерного неравенства в разных контекстах и необходимость применения гендерно ориентированных подходов к борьбе с киберпреступностью. Во-вторых, в нашем исследовании подчеркивается ключевая роль социально-экономических факторов в распространении киберпреступности, особенно в Нигерии. Распространенность киберпреступлений, особенно в сфере электронного банкинга/мошенничества с платежными картами, свидетельствует о социально-экономической динамике в сфере киберпреступности в Нигерии и подчеркивает центральную роль данной категории киберпреступлений в этой стране. В-третьих, мы рассмотрели взаимосвязь между уровнем образования и уязвимостью к онлайн-мошенничеству. Хотя более 99 % наших участников имели высшее образование, распределение по уровням образования

было различным, что повлияло на подверженность киберпреступности. Наши выводы согласуются с существующими исследованиями (Whitty, 2018), указывающими на сложную взаимосвязь между уровнем образования и жертвами мошенничества. И последнее, но не менее важное: учитывая социально-экономический разрыв между Севером и Югом, мы рассмотрели проблему виктимизации в результате киберпреступности с точки зрения концепции идеальной жертвы. Опираясь на фундаментальную работу Christie (1986), мы изучили динамику роста числа жертв онлайн-мошенничества в Нигерии, обращая внимание на различия в уровне интереса исследователей и глобальных мер реагирования на киберпреступления, затрагивающие незападные страны. Наши выводы подчеркивают необходимость применения тщательно выверенных гендерных, инклюзивных и контекстуальных подходов к исследованию киберпреступности и разработке политики в Нигерии и за ее пределами, учитывая обсуждаемую динамику глобальной расстановки сил. Эти выводы показывают актуальность разработки многоаспектных и учитывающих контекст подходов к борьбе с киберпреступностью и смягчению ее последствий для уязвимых групп населения во всем мире.

Список литературы

Aborisade, R. A. (2023). Yahoo boys, yahoo parents? An explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. *Deviant Behavior*, *44*(7), 1102–1120. https://doi.org/10.1080/01639625.2022.2144779

Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology*, *3*, 100044. https://doi.org/10.1016/j.jeconc.2023.100044

Adeduntan, A. (2022). Rhyme, reason, rogue: Yoruba popular music and the hip hop amoral turn. *Journal of Popular Music Studies*, *34*(1), 44–67. https://doi.org/10.1525/jpms.2022.34.1.44

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, *58*(5), 1083–1097. https://doi.org/10.1177/0022343320964549

Akoto, W. (2024). Who spies on whom? Unravelling the puzzle of state-sponsored cyber economic espionage. *Journal of Peace Research*, *61*(1), 59–71. https://doi.org/10.1177/00223433231214417

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. https://doi.org/10.1089/cyber.2010.0307

Button, M., Hock, B., Shepherd, D., & Gilmour, P. (2023). Understanding the rise of fraud in England and Wales through field theory: Blip or flip? *Journal of Economic Criminology*, *1*, 100012. https://doi.org/10.1016/j.jeconc.2023.100012

Button, M., Nicholls, C. M, Kerr, J., & Owen, R. (2015). Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice? *The Howard Journal of Criminal Justice*, *54*(2), 193–211. https://doi.org/10.1111/hojo.12123

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391–408. https://doi.org/10.1177/0004865814521224

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, *64*, 101675. https://doi.org/10.1016/j.tele.2021.101675

Christie, N. (1986). The ideal victim. In E. A. Fattah (Ed.), *From crime policy to victim policy* (pp. 17–30). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-08305-3_2

Cross, C. (2018a). Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave Handbook of Criminology and the Global South* (pp. 261–280). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-65021-0_14

Cross, C. (2018b). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, *55*, 1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, *20*(3), 358–375. https://doi.org/10.1177/1748895819835910

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, *108*, 106310. https://doi.org/10.1016/j.chb.2020.106310

Drew, J. M., & Webster, J. (2024). The victimology of online fraud: A focus on romance fraud victimisation. *Journal of Economic Criminology*, *3*, 100053. https://doi.org/10.1016/j.jeconc.2024.100053

Genc, Y., Kour, H., Arslan, H. T., & Chen, L. C. (2021). Understanding Nigerian e-mail scams: A computational content analysis approach. *Information Security Journal: A Global Perspective*, *30*(2), 88–99. https://doi.org/10.1080/19393555.2020.1804647

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*, 13–20. https://doi.org/10.1007/s11416-006-0015-z

Hall, T., & Yarwood, R. (2024). New geographies of crime? Cybercrime, southern criminology and diversifying research agendas. *Progress in Human Geography*, *48*(4), 437–457. https://doi.org/10.1177/03091325241246015

Harper, C. A., Smith, L., Leach, J., Daruwala, N. A., & Fido, D. (2023). Development and Validation of the Beliefs About Revenge Pornography Questionnaire. *Sexual Abuse*, *35*(6), 748–783. https://doi.org/10.1177/10790632221082663

Hock, B., & Button, M. (2023). Non-ideal victims or offenders? The curious case of pyramid scheme participants. *Victims and Offenders*, *18*(7), 1311–1334. https://doi.org/10.1080/15564886.2023.2186996

Ibrahim, S. (2016a). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Ibrahim, S. (2016b). Causes of socioeconomic cybercrime in Nigeria. In *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada (pp. 1–9). IEEE. https://doi.org/10.1109/icccf.2016.7740439

Idem, U. J. (2023). The Legal Approach for Fighting Cybercrimes in Nigeria: Some Lessons from the United States and the United Kingdom. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 191–198). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050983

Idem, U. J., & Olarinde, E. S. (2023). Cybercrime and its Negative Effects on Youth's Development, the Economy and Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 199–204). IEEE. https://doi.org/10.1109/cymaen57228.2023.10051047

Idem, U. J., Olarinde, E. S., Anwana, E. O., Ogundele, A. T., Awodiran, M. A., & Omomen, M. A. (2023a). The Prosecution of Cybercrimes in Nigeria: Challenges and Prospects. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 178–183). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050896

Idem, U. J., Olarinde, E. S., Ikpeze, N. G., Emem, O., Ogundele, A. T., & Awodiran, M. A. (2023b). Cybercrime Regulatory Agencies need urgent Reform to Protect Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 184–190). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050994

Jaishankar, K. (2011). Introduction: Expanding Cyber Criminology with an Avant-Garde Anthology. In *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. xxvii–xxxv). Boca Raton: CRC Press.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, *1*(1), 1–6. https://doi.org/10.5281/zenodo.18276

Jaishankar, K. (2018). Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology*, *12*(1), 1–8. https://doi.org/10.5281/zenodo.1467308

Kadoya, Y., Khan, M. S. R., Narumoto, J., & Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. *Frontiers in Psychology*, *12*, 649565. https://doi.org/10.3389/fpsyg.2021.649565

Lazarus, S. (2019). Where is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth. *Religions*, *10*(3), 146. https://doi.org/10.3390/rel10030146

Lazarus, S. (2024). Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the «Black Axe» Confraternity. *Deviant Behavior*, 1–25. https://doi.org/10.1080/01639625.2024.2352049

Lazarus, S., & Button, M. (2022). Tweets and Reactions: Revealing the Geographies of Cybercrime Perpetrators and the North-South Divide. *Cyberpsychology, Behavior, and Social Networking*, *25*(8), 504–511. https://doi.org/10.1089/cyber.2021.0332

Lazarus, S., & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, *40*, 14–26. https://doi.org/10.1016/j.tele.2019.04.009

Lazarus, S., Button, M., & Adogame, A. (2022a). Advantageous Comparison: Using Twitter Responses to Understand Similarities between Cybercriminals ("Yahoo Boys") and Politicians ("Yahoo men"). *Heliyon*, *8*(11), e11142. https://doi.org/10.1016/j.heliyon.2022.e11142

Lazarus, S., Button, M., & Kapend, R. (2022b). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice*, *61*(3), 381–398. https://doi.org/10.1111/hojo.12485

Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023). Cheques or Dating Scams? Online Fraud Themes in Hip-Hop Songs Across Popular Music Apps. *Journal of Economic Criminology*, *2*, 100033. https://doi.org/10.1016/j.jeconc.2023.100033

Loyens, K., & Paraciani, R. (2023). Who is the ("Ideal") Victim of Labor Exploitation? Two Qualitative Vignette Studies on Labor Inspectors' Discretion. *The Sociological Quarterly*, *64*(1), 27–45. https://doi.org/10.1080/00380253.2021.1974321

Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. *Journal of Peace Research*, *61*(1), 72–86. https://doi.org/10.1177/00223433231220264

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017, April). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 1301–1310). https://doi.org/10.1145/3041021.3053892

McGerty, L. J. (2000). "Nobody lives only in cyberspace": Gendered subjectivities and domestic use of the Internet. *CyberPsychology & Behavior*, *3*(5), 895–899. https://doi.org/10.1089/10949310050191863

Meikle, W., & Cross, C. (2024). "What action should I take?": Help-seeking behaviours of those targeted by romance fraud. *Journal of Economic Criminology*, *3*, 100054. https://doi.org/10.1016/j.jeconc.2024.100054

Monsurat, I. (2020). African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: a study of the Yahoo Boys in Ilorin, Nigeria. *International Journal of Cyber Criminology*, *14*(1), 300–315. https://doi.org/10.5281/zenodo.3755848

Mosbah-Natanson, S., & Gingras, Y. (2014). The globalization of social sciences? Evidence from a quantitative analysis of 30 years of production, collaboration and citations in the social sciences (1980–2009). *Current Sociology*, *62*(5), 626–646. https://doi.org/10.1177/0011392113498866

Murça, A., Cunha, O., & Almeida, T. C. (2024). Prevalence and Impact of Revenge Pornography on a Sample of Portuguese Women. *Sexuality & Culture*, *28*(1), 96–112. https://doi.org/10.1007/s12119-023-10100-3

Musotto, R., & Wall, D. S. (2020). More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. *Trends in Organized Crime*, *25*, 173–191. https://doi.org/10.1007/s12117-020-09397-5

Näsi, M., Danielsson, P., & Kaakinen, M. (2023). Cybercrime Victimisation and Polyvictimisation in Finland – Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*, *29*, 283–301. https://doi.org/10.1007/s10610-021-09497-0

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, *34*, 231–245. https://doi.org/10.1007/s11896-019-09334-5

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology*, *13*(2). https://doi.org/10.5281/zenodo.3702333

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, *6*(2), 1001–1013.

Ojolo, T. L., & Singh, S. B. (2023). Interrogating the Yahoo-Yahoo Menace: An Analysis of Moral Decadence, Poverty, and Unemployment In Nigeria. *Journal of African Films and Diaspora Studies*, *6*(1), 55. https://doi.org/10.31920/2516-2713/2023/6n1a4

Ojolo, T., & Adewumi, S. A. (2020). Understanding youths' perception and factors advancing cybercrime (yahoo-yahoo) in Ado-Ekiti, Ekiti State, Nigeria. *African Journal of Gender, Society & Development*, *9*(4), 243. https://doi.org/10.31920/2634-3622/2020/v9n4a11

Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, *36*(2), 350–372. https://doi.org/10.1057/s41284-022-00342-5

Olaiya, T. A., Lamidi, K. O., & Bello, M. A. (2020). Narrative of illicit money: 'Yahoo'Boy (Format) of cyber scams and governance challenges in Africa. *Global Journal of Interdisciplinary Social Sciences*, *9*(2), 003.

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, *43*(4), 626–642. https://doi.org/10.1016/j.ijlcj.2015.02.003

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. New Delhi: Routledge. https://doi.org/10.4324/9781315205786

Rich, T. (2018). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal*, *31*, 208–225. https://doi.org/10.1057/s41284-017-0095-0

Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, *37*(2), 209–215. https://doi.org/10.1016/j.jcrimjus.2009.02.003

Tade, O., & Adeniyi, O. (2017). 'They withdrew all I was worth': Automated teller machine fraud and victims' life chances in Nigeria. *International Review of Victimology*, *23*(3), 313–324. https://doi.org/10.1177/0269758017704330

Tao, H. (2022). Loving strangers, avoiding risks: Online dating practices and scams among Chinese lesbian (lala) women. *Media, Culture & Society*, *44*(6), 1199–1214. https://doi.org/10.1177/01634437221088952

Timofeyev, Y., & Dremova, O. (2022). Insurers' responses to cyber crime: evidence from Russia. *International Journal of Law, Crime and Justice*, *68*, 100520. https://doi.org/10.1016/j.ijlcj.2021.100520

Wang, F. (2023). Sentencing Disparity and Focal Concern: An Assessment of Judicial Decisions on Sha Zhu Pan Cases Collected From China Judgements Online. *Crime & Delinquency*, *0*(0). https://doi.org/10.1177/00111287231158571

Wang, F., & Topalli, V. (2024). Understanding romance scammers through the lens of their victims: qualitative modeling of risk and protective factors in the online context. *American Journal of Criminal Justice*, *49*(1), 145–181. https://doi.org/10.1007/s12103-022-09706-4

Weijer van de, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*, *43*(1), 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

Whittaker, J. M., Lazarus, S., & Corcoran, T. (2024). Are fraud victims nothing more than animals? Critiquing the propagation of "pig butchering" (Sha Zhu Pan, 杀猪盘). *Journal of Economic Criminology*, *3*, 100052. https://doi.org/10.1016/j.jeconc.2024.100052

Whitty, M. (2018). Do you love me? Psychological characteristics of Romance scam victims. *Cyberpsychology Behavior and Social Networking*, *21*(2), 105–109. https://doi.org/10.1089/cyber.2016.0729

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/jfc-10-2017-0095

Сведения об авторах

Амину Мухаммад Аувал – бакалавр в области информационных технологий, специалист в области информационных технологий, Университет Джоса
Адрес: Нигерия, PMB 2084, штат Плато, г. Джос
E-mail: i.elameenu@gmail.com
ORCID ID: https://orcid.org/0009-0005-1799-7876
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JFS-7098-2023
Google Scholar ID: https://scholar.google.com/citations?user=RDxPEr4AAAAJ

Сулеман Лазарус – PhD в области киберпреступности и криминологии, приглашенный специалист Центра криминологии им. Маннхайма, Лондонская школа экономики и политических наук; сотрудник Центра изучения старения населения, университет Суррея; почетный преподаватель Центра по изучению киберпреступности и экономической преступности, Портсмутский университет
Адрес: Великобритания, WC2A 2AE, г. Лондон, Хьютон Стрит; Великобритания GU2 7XH, г. Гилфорд, Стэг Хилл; Великобритания, PO1 2HY, г. Портсмут, Сент-Джордж Билдинг.
E-mail: suleman.lazarus@gmail.com
ORCID ID: https://orcid.org/0000-0003-1721-8519
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57205679641
WoS Researcher ID: https://www.webofscience.com/wos/author/record/629543
Google Scholar ID: https://scholar.google.com/citations?user=Em8EXqcAAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.81 / Криминология
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 16 мая 2024 г.
Дата одобрения после рецензирования – 28 мая 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:343.9:004.8
EDN: https://elibrary.ru/jvglrh
DOI: https://doi.org/10.21202/jdtl.2024.44

Sociological and Criminological Research of Victimization Issues: Preliminary Stage and New Sphere of Cybercrime Categorization

Aminu Muhammad Auwal
University of Jos, Jos, Nigeria

Suleman Lazarus ✉
London School of Economics and Political Science, London, United Kingdom
University of Surrey, Guildford, United Kingdom
University of Portsmouth, Portsmouth, United Kingdom

Keywords

cybercrime victim,
cybercrime,
cybercriminology,
cyber-espionage,
digital criminology,
digital technologies,
legal policy,
online fraud,
victimization,
victimology

Abstract

Objective: to identify the main issues of victimization as a result of cybercrime growth in the world in general and in Nigerian society in particular from the standpoint of sociological approaches, using a Tripartite Cybercrime Framework (TCF), which comprises geopolitical, psychosocial and socio-economic categories of cybercrime.

Methods: the methodology is based on the sociological research method. The data collection included the distribution of a questionnaire among 896 participants from the academic environment, including students and university staff, and the analysis of the responses. The presented data were analyzed using descriptive statistics, with special attention to the issues of gender inequality, socio-economic factors, the impact of educational level on vulnerability to online fraud and victimization as a result of cybercrime through the prism of the ideal victim concept and the socio-economic gap between North and South.

Results: the article presents an analysis of the Tripartite Cybercrime Framework. The survey showed that 65.20% of the participants had been victims of cybercrime. There were more men among the victims (64.69%). The authors found patterns in the distribution of cybercrimes. All cybercrimes against the respondent were socio-economic ones, which underlines the

✉ Corresponding author

high frequency of cybercrime and the relevance of countering it in Nigerian society. Special attention was paid to the issues of gender inequality, socio-economic factors, and the impact of education on vulnerability to cybercrime. The article considers from the viewpoint of the ideal victim concept. The study results provide an idea of the prevalence and distribution of specific types of cybercrime in the socio-economic category among the studied population.

Scientific novelty: For the first time, the study uses the Tripartite Cybercrime Framework (TCF) to study victimization as a result of cybercrime in Nigerian society. The research novelty is also due to the fact that the conceptual foundations of countering cybercrime that have developed in the global North are not fully applicable in Nigeria.

Practical significance: the results obtained demonstrate the need to apply carefully calibrated gender-based, inclusive and contextual approaches to the development of a national legal policy to combat cybercrime. The results can be used to justify the law-making decisions which are being developed in the field of preventing and countering manifestations of cybercrime, as well as to form the basis for legal measures to protect cybercrime victims.

For citation

Auwal, A. M., & Lazarus, S. (2024). Sociological and Criminological Research of Victimization Issues: Preliminary Stage and New Sphere of Cybercrime Categorization. *Journal of Digital Technologies and Law, 2*(4), 915–942. https://doi.org/10.21202/jdtl.2024.44

References

Aborisade, R. A. (2023). Yahoo boys, yahoo parents? An explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. *Deviant Behavior*, *44*(7), 1102–1120. https://doi.org/10.1080/01639625.2022.2144779

Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology*, *3*, 100044. https://doi.org/10.1016/j.jeconc.2023.100044

Adeduntan, A. (2022). Rhyme, reason, rogue: Yoruba popular music and the hip hop amoral turn. *Journal of Popular Music Studies*, *34*(1), 44–67. https://doi.org/10.1525/jpms.2022.34.1.44

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, *58*(5), 1083–1097. https://doi.org/10.1177/0022343320964549

Akoto, W. (2024). Who spies on whom? Unravelling the puzzle of state-sponsored cyber economic espionage. *Journal of Peace Research*, *61*(1), 59–71. https://doi.org/10.1177/00223433231214417

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. https://doi.org/10.1089/cyber.2010.0307

Button, M., Hock, B., Shepherd, D., & Gilmour, P. (2023). Understanding the rise of fraud in England and Wales through field theory: Blip or flip? *Journal of Economic Criminology*, *1*, 100012. https://doi.org/10.1016/j.jeconc.2023.100012

Button, M., Nicholls, C. M, Kerr, J., & Owen, R. (2015). Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice? *The Howard Journal of Criminal Justice*, *54*(2), 193–211. https://doi.org/10.1111/hojo.12123

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391–408. https://doi.org/10.1177/0004865814521224

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, *64*, 101675. https://doi.org/10.1016/j.tele.2021.101675

Christie, N. (1986). The ideal victim. In E. A. Fattah (Ed.), *From crime policy to victim policy* (pp. 17–30). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-08305-3_2

Cross, C. (2018a). Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave Handbook of Criminology and the Global South* (pp. 261–280). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-65021-0_14

Cross, C. (2018b). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, *55*, 1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, *20*(3), 358–375. https://doi.org/10.1177/1748895819835910

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, *108*, 106310. https://doi.org/10.1016/j.chb.2020.106310

Drew, J. M., & Webster, J. (2024). The victimology of online fraud: A focus on romance fraud victimisation. *Journal of Economic Criminology*, *3*, 100053. https://doi.org/10.1016/j.jeconc.2024.100053

Genc, Y., Kour, H., Arslan, H. T., & Chen, L. C. (2021). Understanding Nigerian e-mail scams: A computational content analysis approach. *Information Security Journal: A Global Perspective*, *30*(2), 88–99. https://doi.org/10.1080/19393555.2020.1804647

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*, 13–20. https://doi.org/10.1007/s11416-006-0015-z

Hall, T., & Yarwood, R. (2024). New geographies of crime? Cybercrime, southern criminology and diversifying research agendas. *Progress in Human Geography*, *48*(4), 437–457. https://doi.org/10.1177/03091325241246015

Harper, C. A., Smith, L., Leach, J., Daruwala, N. A., & Fido, D. (2023). Development and Validation of the Beliefs About Revenge Pornography Questionnaire. *Sexual Abuse*, *35*(6), 748–783. https://doi.org/10.1177/10790632221082663

Hock, B., & Button, M. (2023). Non-ideal victims or offenders? The curious case of pyramid scheme participants. *Victims and Offenders*, *18*(7), 1311–1334. https://doi.org/10.1080/15564886.2023.2186996

Ibrahim, S. (2016a). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Ibrahim, S. (2016b). Causes of socioeconomic cybercrime in Nigeria. In *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada (pp. 1–9). IEEE. https://doi.org/10.1109/icccf.2016.7740439

Idem, U. J. (2023). The Legal Approach for Fighting Cybercrimes in Nigeria: Some Lessons from the United States and the United Kingdom. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 191–198). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050983

Idem, U. J., & Olarinde, E. S. (2023). Cybercrime and its Negative Effects on Youth's Development, the Economy and Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 199–204). IEEE. https://doi.org/10.1109/cymaen57228.2023.10051047

Idem, U. J., Olarinde, E. S., Anwana, E. O., Ogundele, A. T., Awodiran, M. A., & Omomen, M. A. (2023a). The Prosecution of Cybercrimes in Nigeria: Challenges and Prospects. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 178–183). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050896

Idem, U. J., Olarinde, E. S., Ikpeze, N. G., Emem, O., Ogundele, A. T., & Awodiran, M. A. (2023b). Cybercrime Regulatory Agencies need urgent Reform to Protect Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 184–190). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050994

Jaishankar, K. (2011). Introduction: Expanding Cyber Criminology with an Avant-Garde Anthology. In *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. xxvii–xxxv). Boca Raton: CRC Press.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, *1*(1), 1–6. https://doi.org/10.5281/zenodo.18276

Jaishankar, K. (2018). Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology*, *12*(1), 1–8. https://doi.org/10.5281/zenodo.1467308

Kadoya, Y., Khan, M. S. R., Narumoto, J., & Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. *Frontiers in Psychology*, *12*, 649565. https://doi.org/10.3389/fpsyg.2021.649565

Lazarus, S. (2019). Where is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth. *Religions*, *10*(3), 146. https://doi.org/10.3390/rel10030146

Lazarus, S. (2024). Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the «Black Axe» Confraternity. *Deviant Behavior*, 1–25. https://doi.org/10.1080/01639625.2024.2352049

Lazarus, S., & Button, M. (2022). Tweets and Reactions: Revealing the Geographies of Cybercrime Perpetrators and the North-South Divide. *Cyberpsychology, Behavior, and Social Networking*, *25*(8), 504–511. https://doi.org/10.1089/cyber.2021.0332

Lazarus, S., & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, *40*, 14–26. https://doi.org/10.1016/j.tele.2019.04.009

Lazarus, S., Button, M., & Adogame, A. (2022a). Advantageous Comparison: Using Twitter Responses to Understand Similarities between Cybercriminals ("Yahoo Boys") and Politicians ("Yahoo men"). *Heliyon*, *8*(11), e11142. https://doi.org/10.1016/j.heliyon.2022.e11142

Lazarus, S., Button, M., & Kapend, R. (2022b). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice*, *61*(3), 381–398. https://doi.org/10.1111/hojo.12485

Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023). Cheques or Dating Scams? Online Fraud Themes in Hip-Hop Songs Across Popular Music Apps. *Journal of Economic Criminology*, *2*, 100033. https://doi.org/10.1016/j.jeconc.2023.100033

Loyens, K., & Paraciani, R. (2023). Who is the ("Ideal") Victim of Labor Exploitation? Two Qualitative Vignette Studies on Labor Inspectors' Discretion. *The Sociological Quarterly*, *64*(1), 27–45. https://doi.org/10.1080/00380253.2021.1974321

Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. *Journal of Peace Research*, *61*(1), 72–86. https://doi.org/10.1177/00223433231220264

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017, April). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 1301–1310). https://doi.org/10.1145/3041021.3053892

McGerty, L. J. (2000). "Nobody lives only in cyberspace": Gendered subjectivities and domestic use of the Internet. *CyberPsychology & Behavior*, *3*(5), 895–899. https://doi.org/10.1089/10949310050191863

Meikle, W., & Cross, C. (2024). "What action should I take?": Help-seeking behaviours of those targeted by romance fraud. *Journal of Economic Criminology*, *3*, 100054. https://doi.org/10.1016/j.jeconc.2024.100054

Monsurat, I. (2020). African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: a study of the Yahoo Boys in Ilorin, Nigeria. *International Journal of Cyber Criminology*, *14*(1), 300–315. https://doi.org/10.5281/zenodo.3755848

Mosbah-Natanson, S., & Gingras, Y. (2014). The globalization of social sciences? Evidence from a quantitative analysis of 30 years of production, collaboration and citations in the social sciences (1980–2009). *Current Sociology*, *62*(5), 626–646. https://doi.org/10.1177/0011392113498866

Murça, A., Cunha, O., & Almeida, T. C. (2024). Prevalence and Impact of Revenge Pornography on a Sample of Portuguese Women. *Sexuality & Culture*, *28*(1), 96–112. https://doi.org/10.1007/s12119-023-10100-3

Musotto, R., & Wall, D. S. (2020). More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. *Trends in Organized Crime*, *25*, 173–191. https://doi.org/10.1007/s12117-020-09397-5

Näsi, M., Danielsson, P., & Kaakinen, M. (2023). Cybercrime Victimisation and Polyvictimisation in Finland – Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*, *29*, 283–301. https://doi.org/10.1007/s10610-021-09497-0

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, *34*, 231–245. https://doi.org/10.1007/s11896-019-09334-5

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology*, *13*(2). https://doi.org/10.5281/zenodo.3702333

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, *6*(2), 1001–1013.

Ojolo, T. L., & Singh, S. B. (2023). Interrogating the Yahoo-Yahoo Menace: An Analysis of Moral Decadence, Poverty, and Unemployment In Nigeria. *Journal of African Films and Diaspora Studies*, *6*(1), 55. https://doi.org/10.31920/2516-2713/2023/6n1a4

Ojolo, T., & Adewumi, S. A. (2020). Understanding youths' perception and factors advancing cybercrime (yahoo-yahoo) in Ado-Ekiti, Ekiti State, Nigeria. *African Journal of Gender, Society & Development*, *9*(4), 243. https://doi.org/10.31920/2634-3622/2020/v9n4a11

Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, *36*(2), 350–372. https://doi.org/10.1057/s41284-022-00342-5

Olaiya, T. A., Lamidi, K. O., & Bello, M. A. (2020). Narrative of illicit money: 'Yahoo'Boy (Format) of cyber scams and governance challenges in Africa. *Global Journal of Interdisciplinary Social Sciences*, *9*(2), 003.

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, *43*(4), 626–642. https://doi.org/10.1016/j.ijlcj.2015.02.003

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. New Delhi: Routledge. https://doi.org/10.4324/9781315205786

Rich, T. (2018). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal*, *31*, 208–225. https://doi.org/10.1057/s41284-017-0095-0

Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, *37*(2), 209–215. https://doi.org/10.1016/j.jcrimjus.2009.02.003

Tade, O., & Adeniyi, O. (2017). 'They withdrew all I was worth': Automated teller machine fraud and victims' life chances in Nigeria. *International Review of Victimology*, *23*(3), 313–324. https://doi.org/10.1177/0269758017704330

Tao, H. (2022). Loving strangers, avoiding risks: Online dating practices and scams among Chinese lesbian (lala) women. *Media, Culture & Society*, *44*(6), 1199–1214. https://doi.org/10.1177/01634437221088952

Timofeyev, Y., & Dremova, O. (2022). Insurers' responses to cyber crime: evidence from Russia. *International Journal of Law, Crime and Justice*, *68*, 100520. https://doi.org/10.1016/j.ijlcj.2021.100520

Wang, F. (2023). Sentencing Disparity and Focal Concern: An Assessment of Judicial Decisions on Sha Zhu Pan Cases Collected From China Judgements Online. *Crime & Delinquency*, *0*(0). https://doi.org/10.1177/00111287231158571

Wang, F., & Topalli, V. (2024). Understanding romance scammers through the lens of their victims: qualitative modeling of risk and protective factors in the online context. *American Journal of Criminal Justice*, *49*(1), 145–181. https://doi.org/10.1007/s12103-022-09706-4

Weijer van de, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*, *43*(1), 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

Whittaker, J. M., Lazarus, S., & Corcoran, T. (2024). Are fraud victims nothing more than animals? Critiquing the propagation of "pig butchering" (Sha Zhu Pan, 杀猪盘). *Journal of Economic Criminology*, *3*, 100052. https://doi.org/10.1016/j.jeconc.2024.100052

Whitty, M. (2018). Do you love me? Psychological characteristics of Romance scam victims. *Cyberpsychology Behavior and Social Networking*, *21*(2), 105–109. https://doi.org/10.1089/cyber.2016.0729

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/jfc-10-2017-0095

Authors information

Aminu Muhammad Auwal – Bachelor of Science in Information Technology, IT Specialist, University of Jos
Address: PMB 2084, Jos, Plateau State, Nigeria
E-mail: i.elameenu@gmail.com
ORCID ID: https://orcid.org/0009-0005-1799-7876
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JFS-7098-2023
Google Scholar ID: https://scholar.google.com/citations?user=RDxPEr4AAAAJ

Suleman Lazarus – PhD in Cybercrime and Criminology, Visiting Fellow at the Mannheim Centre for Criminology, London School of Economics and Political Science; Fellow at the Centre of Excellence on Ageing, University of Surrey; Honorary Lecturer at the Centre for Cybercrime and Economic Crime, University of Portsmouth.
Address: Houghton Street, London, WC2A 2AE, United Kingdom; Stag Hill, Guildford, GU2 7XH, United Kingdom; St. George's Building, Portsmouth, PO1 2HY, United Kingdom.
E-mail: suleman.lazarus@gmail.com
ORCID ID: https://orcid.org/0000-0003-1721-8519
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57205679641
WoS Researcher ID: https://www.webofscience.com/wos/author/record/629543
Google Scholar ID: https://scholar.google.com/citations?user=Em8EXqcAAAAJ

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 16, 2024
Date of approval – May 28, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024