



Научная статья

УДК 34:004:343.3/.7:341.4:343.9

EDN: <https://elibrary.ru/cmvmqzx>

DOI: <https://doi.org/10.21202/jdtl.2023.43>

Применение концепции «обязанность защищать» (R2P) для введения универсальной юрисдикции в отношении кибертерроризма

Яссин Абдалла Абделькарим

Суд общей юрисдикции в Луксоре

г. Сохаг, Египет

Ключевые слова

кибербезопасность,
киберпространство,
кибертерроризм,
международное публичное
право,
международное частное
право,
права человека,
право,
преступления против
человечности,
цифровые технологии,
юрисдикция

Аннотация

Цель: развитие беспроводных технологий и цифровой инфраструктуры радикальным образом изменило среду обитания человечества, порождая новый тип пространства – киберпространство. Уникальность и особенности этой среды, включая анонимность, безграничность, проблемы, связанные с определением и установлением юрисдикции, стали питательной средой для появления новой глобальной угрозы – кибертерроризма, характеризующегося высоким уровнем латентности, низким уровнем раскрываемости и несравнимо большей опасностью, нежели преступления «в реальном мире». Противодействие новым формам преступности потребовало разработки универсальных инструментов, преодолевающих ограничения традиционной юрисдикции и позволяющих государствам преследовать террористов в киберпространстве. Определение соответствующих инструментов и выявление препятствий политико-юридического характера по их реализации является целью проведенного исследования.

Методы: для достижения поставленной цели используется, прежде всего, формально-юридический метод, применяемый для анализа правовых источников, к которым относятся судебная практика, национальное законодательство и международные акты. Также был задействован доктринальный подход, позволивший на основе научных трудов и теоретических конструкций объяснить сложность новых явлений современного мира и спрогнозировать их развитие в будущем. Основное внимание при этом уделяется стороне преступника, чтобы доказать ее антагонизм с человечеством в соответствии с теоретическими взглядами. Наконец, в исследовании анализируются теории универсальной и традиционной юрисдикции, а также то, как они применяются для преследования террористов.

© Абделькарим Я. А., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Результаты: в работе дается критический анализ переосмысления и адаптации концепции юрисдикции применительно к глобальной, безграничной и децентрализованной цифровой среде (киберпространство) и противодействию новым формам терроризма (кибертерроризм); приводятся различные юрисдикционные модели, применимые в киберпространстве; преодолевается разрыв между основными отраслями права: международным частным и публичным правом – путем установления взаимосвязи в отношении к кибертерроризму двух теорий: концепций «обязанности защищать» (R2P) и применения универсальной юрисдикции; выявлены тенденции развития универсальной юрисдикции.

Научная новизна: исследование развивает накопленные научные знания в части обоснования введения иностранной юрисдикции на территории государства для преследования кибертеррористов; устанавливается связь между теориями универсальной юрисдикции в международном частном праве и «обязанностью защищать» (R2P) в международном публичном праве; при этом последняя признается в качестве пригодной основы для введения универсальной юрисдикции в отношении кибертерроризма; переосмысливаются такие традиционные понятия, как суверенитет и юрисдикционная независимость. Устраняется пробел в знаниях, связанных с рассмотрением кибертерроризма как преступления против человечности в международном праве.

Практическая значимость: реализация предложенных выводов будет способствовать усилению международного преследования кибертерроризма; гармонизации международного и внутригосударственного правового инструментария в отношении данного преступления.

Для цитирования

Абделькарим, Я. А. (2023). Применение концепции «обязанность защищать» (R2P) для введения универсальной юрисдикции в отношении кибертерроризма. *Journal of Digital Technologies and Law*, 1(4), 994–1022. <https://doi.org/10.21202/jdtl.2023.43>

Содержание

Введение

1. Превентивный характер концепции «обязанность защищать» (R2P) в отношении преступлений против человечности (ППЧ)
 - 1.1. Унификация концепции R2P для предотвращения ППЧ
 - 1.2. Применение R2P в международном праве
2. Правовые основы для отнесения кибертерроризма к категории «Другие бесчеловечные деяния» согласно Римскому статуту
 - 2.1. Анализ кибертерроризма
 - 2.2. Контекстуальные элементы преступлений против человечности: другие бесчеловечные деяния
 - 2.3. Применимость категории «другие бесчеловечные деяния» к кибертерроризму
3. Универсальная юрисдикция для преследования ППЧ
 - 3.1. Принцип *aut dedere aut judicare* в отношении кибертерроризма

4. Заполнение пробела в законодательстве

4.1. Объяснение существующей дилеммы

4.2. Решение: применимость концепции R2P для введения универсальной юрисдикции в отношении кибертерроризма

Заключение

Список литературы

Введение

Ученые всего мира признают, что концепция «обязанность защищать» предусматривает необходимость защиты прав человека. Кроме того, не вызывает сомнений глобальный характер потенциальных разрушений в результате кибертерроризма. Следовательно, упомянутая теория является адекватным основанием для введения универсальной юрисдикции в отношении кибертерроризма. В настоящей статье представлена концепция «обязанность защищать» (англ. “responsibility to protect”, далее – R2P), которая обосновывает введение универсальной юрисдикции в отношении кибертерроризма. Автор показывает связь между двумя теориями международного права: теорией универсальной юрисдикции в рамках международного частного права и концепцией «обязанность защищать» в рамках международного публичного права.

Исследование вносит вклад в науку, предлагая международному сообществу правовое обоснование введения иностранной юрисдикции на территории государства для преследования кибертеррористов. Установлена связь между теорией универсальной юрисдикции в международном частном праве и концепцией «обязанность защищать» в международном публичном праве. Таким образом, преодолевается разрыв между этими основными отраслями международного права. Кроме того, работа задает новый контекст традиционным понятиям, например, понятиям суверенитета и юрисдикционной независимости, для достижения ранее поставленных целей гуманитарных наук. Исследование также устраняет пробел в науке, связывая кибертерроризм с известной в международном праве концепцией преступлений против человечности (далее – ППЧ); автор доказывает применимость элементов последней к кибертерроризму как международной противоправной деятельности. Таким образом, теория R2P может способствовать установлению универсальной юрисдикции в отношении кибертерроризма, как это происходит в отношении ППЧ.

В работе анализируется структура кибертерроризма и исследуются его скрытые элементы в условиях неоднозначности киберпространства. Безграничность последнего требует разработки инструмента, преодолевающего ограничения традиционной юрисдикции. Таким инструментом является универсальная юрисдикция, позволяющая государствам преследовать террористов в киберпространстве независимо от их местонахождения. Однако ее применение наталкивается на препятствия как юридического, так и политического характера. Поэтому эффективным средством поддержки этого инструмента должна стать теория, включающая ряд обязательных элементов.

Проведенное исследование должно поспособствовать развитию уголовного преследования кибертерроризма во всем мире, поскольку обосновывает использование международного правового инструментария против этого преступления. Доказывается, что кибертерроризм – это преступление против человечности, требующее международного вмешательства в соответствии с теорией R2P, которая представлена как регулятивная правовая норма. Автор показывает необходимость для всех стран сплотиться ради предотвращения этих тяжких преступлений в соответствии

с нормами Устава ООН путем гармонизации международного и внутригосударственного правового инструментария в отношении данного преступления. Таким образом, международное право способно выступить против кибертерроризма и искоренить его в киберпространстве.

Методология. Для достижения поставленных целей в исследовании использован теоретический подход. Он основан на доктринальном методе изучения первичных и вторичных источников права с целью анализа встречающихся в них положений. К таким источникам относятся судебная практика, внутреннее законодательство стран и международные правовые акты. Анализ основывается на логических рассуждениях. При таком подходе анализируются нормы, включенные в правовые материалы для выработки правового понимания вопроса исследования. Кроме того, изучены аргументированные обзоры судебной практики и первичных правовых источников.

Обзор научных публикаций по теме позволяет выявить пробелы в знаниях, на устранение которых и направлено исследование. Рассматривается контекст теории R2P, подчеркивается ее цель – защита человечества от преступлений. Далее в работе рассматривается концепция кибертерроризма и доказывается антагонизм преступника по отношению к человечеству. Наконец, в исследовании подвергается критике имеющаяся в литературе информация о теории универсальной юрисдикции и о том, как она применяется для преследования террористов в различных юрисдикциях.

Кроме того, проанализированы источники международного и национального права с целью изучения того, как теория универсальной юрисдикции используется при преследовании кибертеррористов. В статье описаны соответствующие тенденции в отношении данной теории.

1. Превентивный характер концепции «обязанность защищать» (R2P) в отношении преступлений против человечности (ППЧ)

В международном праве постулируется безусловная обязанность государств защищать человечество от злодеяний. Международный пакт о гражданских и политических правах и Международный пакт об экономических, социальных и культурных правах указывают основные права человека в качестве объекта такой защиты. Еще в 1948 г. была принята Конвенция о предупреждении преступления геноцида и наказании за него, установившая обязанность государства предотвращать преступления, связанные с геноцидом¹. Кроме того, эти обязанности закреплены в Уставе ООН в целях защиты человечества путем обеспечения мира во всем мире. Постепенно эта доктрина ООН стала восприниматься как защита от ППЧ². В докладе Всемирного саммита 2005 г. четко обозначено, что теория ответственности международного сообщества необходима для достижения целей ООН. Указанные правовые инструменты устанавливают пороговые показатели возникновения обязательств государства. Юридическая сила этих обязательств отражает возможности их соблюдения в рамках глобальной правовой системы и решимость государств защищать человечество. Таким образом, концепция «обязанности защищать» имеет прочные корни в международном праве.

¹ The 1948 Convention on the Prevention and Punishment of the Crime of Genocide, Arts 3, 6 and 8.

² The UN General Assembly. Resolution Adopted by the General Assembly: 60/1 (UN, 2005), para. 139 and the Resolution A/75/277 (UN 2021), para. 6.

1.1. Унификация концепции R2P для предотвращения ППЧ

Таким образом, доктрина устанавливает концепцию R2P в качестве международно-правовой нормы, направленной на предотвращение бесчеловечных злодеяний. Она упоминается в резолюциях Совета безопасности ООН (далее – СБ ООН) для обоснования вмешательства при предотвращении преступлений против человечности³. Такая позиция превращает концепцию R2P из некоей инновационной идеи в общепризнанный правовой принцип международного права. Появляется системная правовая основа для вмешательства при предотвращении ППЧ (Cantini & Zavalov, 2018). ППЧ подразумевают ответственность международного сообщества за принятие мер, независимо от соображений суверенитета. Таким образом, концепция R2P подразумевает содействие мерам по предотвращению преступлений против человечности, предпринимаемым международным сообществом или иностранной юрисдикцией (Cantini & Zavalov, 2018).

По утверждению Ч. Ройера, политическая воля государств и традиционное понимание их суверенитета препятствуют вмешательству международного сообщества для предотвращения ППЧ (Royer, 2021). Поэтому он подчеркивает, что при интерпретации своих национальных интересов в отношении преступлений против человечности государства должны задействовать концепцию R2P (Royer, 2021). По его мнению, концепция R2P не может служить ориентиром для государственной политики, поэтому страны часто выступают против его применения. Это предполагает переосмысление усилий международного сообщества по борьбе с преступлениями. При этом, хотя концепция R2P представляет собой моральную норму, в доктрине она должна рассматриваться как превентивная процедура для защиты человечества (Royer, 2021). Такая интеграция поддерживает роль концепции R2P в международной политике, поскольку исключает экстремистские патриотические настроения, направленные против иностранного вмешательства. Новое понимание концепции R2P, предложенное Ройером, подчеркивает серьезность ППЧ как всеобщего зла, для борьбы с которым необходимо сотрудничество на глобальном уровне.

По мнению С. Уатта, концепция R2P должна быть закреплена в международном праве посредством институтов ООН (Wyatt, 2019). Он утверждает, что данная концепция продолжает политику защиты человечности, принятой ООН, поскольку налагает на государства-члены коллективную ответственность за предотвращение преступлений против человечности (Wyatt, 2019). Кроме того, она расширяет пределы строгого понимания государственного суверенитета в духе Вестфальской системы⁴, дополняя его с точки зрения ответственности. Таким образом, понятия суверенитета и космополитической защиты человечности оказываются связаны моралью. С. Уатт также считает, что органы ООН могут эффективно обеспечить соблюдение правопорядка в соответствии с концепцией R2P, поэтому именно они должны следить за ее применением. Такой конституционный порядок гарантирует эффективную интеграцию обязательств в рамках концепции R2P в международное право и их стабильное исполнение. В этом проявляется солидарная ответственность на глобальном уровне, заложенная в Уставе ООН. Тем самым международная дипломатия и доктрина получают сбалансированную концепцию всеобщей солидарности для поддержания мира

³ Resolutions 1674 (2006), 63/308 (2009)68 and 1894 (2009).

⁴ Там же, р. 99. Суверенитет понимается как «высшая власть на определенной территории».

и безопасности⁵. Такая интерпретация направлена на закрепление концепции R2P в международном праве и дипломатии. Попытка навязать конституционный характер концепции R2P государствам требует их четкого согласия, поскольку может противоречить их трактовке суверенитета. Кроме того, упомянутый баланс подразумевает унификацию взглядов государств на их ответственность, иначе противодействие ППЧ будет рассматриваться как солидарное обязательство в рамках Устава. На практике политические круги противостоят попыткам применить концепцию R2P, считая ее проявлением западного империализма, которому следует оказывать сопротивление из патриотических соображений. Несмотря на то, что интервенция НАТО в Ливию была одобрена СБ ООН в соответствии с концепцией R2P⁶, она подверглась критике, поскольку нарушила государственный суверенитет и привела к политическому хаосу в стране. Это может быть расценено как использование международного правосудия в политических целях. Чтобы решить эту проблему, в международном праве необходимо юридически контекстуализировать концепцию R2P для каждого конкретного случая, чтобы гарантировать ее непредвзятость.

ППЧ со стороны третьих лиц, например террористов, в отношении местного населения влечет за собой обязанность международного сообщества вмешаться с целью предотвращения преступления, если не последовало реакции государства, где это произошло (Soler, 2019). При таком внешнем вмешательстве могут использоваться инструменты иностранной юрисдикции. Здесь объединяются обязанности как государства, так и международного сообщества по предотвращению жестоких злодеяний, нарушающих основные права человека (Park & Switzer, 2020), а правовые процедуры становятся транснациональными⁷. Таким образом, подобные вмешательства обеспечивают достижение целей концепции R2P, поскольку ее гуманитарные аспекты преобладают над соображениями суверенитета. Эта обязанность международного сообщества вызывается невыполнением соответствующим государством своих обязанностей по защите основных прав человека. Кроме того, преступления против человечности не должны использовать государственный суверенитет в качестве щита, позволяющего избежать судебного преследования (Soler, 2019). Более того, международное право допускает гуманитарное вмешательство для предотвращения нарушений прав человека даже с применением силы, хотя и в редких случаях (Azubuike, 2023). Обращение в суд тем более является подходящим решением для защиты этих прав. Эти права закреплены в международном праве, которое предоставляет им постоянную защиту.

Примечательно, что нормы R2P могут быть использованы в киберпространстве для пресечения террористической деятельности и содействовать сотрудничеству крупнейших интернет-компаний и государственных органов в обеспечении ответственных мер для достижения этой цели (Park & Switzer, 2020). Это подтверждает, что концепция R2P может помочь бороться с кибертерроризмом в киберпространстве.

⁵ Там же, p. 156.

⁶ The United Nations Security Council S/RES/1973 (2011), para. 4.

⁷ Kosiba, K. (2018). Is R2P the Remedy for Illegal Deforestation? A Case Study Based on the Systematic Human Rights Violations in Peru. Master of Arts Dissertation submitted to the Brussels School of International Law. University of Kent. <https://clck.ru/36ksvy>

1.2. Применение R2P в международном праве

Международный суд ООН определяет R2P как коллективную обязанность по поддержанию всеобщего мира и безопасности⁸. Таким образом, государства должны использовать доступные им методы для достижения этой цели. По своей сути концепция R2P представляет собой обязательство должной ответственности, поскольку государства не обязаны добиваться полного предотвращения этих преступлений⁹. Эта норма показывает гибкость концепции R2P в международном праве, что делает ее адекватным основанием для применения универсального инструментария, т. е. универсальной юрисдикции, в отношении ППЧ.

Установление ответственности за преступления против человечности расширяет повестку дня Международного уголовного суда (далее – МУС) по обеспечению эффективной защиты человека (Bellamy, 2018). На данном этапе концепция R2P соответствует целям Римского статута, поскольку может быть использована для обеспечения правовой основы инструментария МУС. Концепция использует невоенные превентивные меры МУС для пресечения ППЧ в соответствии со ст. 7 Статута (Holvoet & Mema, 2015). Действительно, МУС оказывается эффективным для достижения этой цели благодаря своим принципам превентивности и постоянства (Holvoet & Mema, 2015). Таким образом, комплексное использование инструментов МУС и R2P сможет эффективно защитить человечество от ППЧ.

Эта гуманитарная цель оправдывает использование данных инструментов даже в отношении государств, не являющихся сторонами Конвенции, особенно при закреплении R2P в резолюциях СБ ООН. Однако для обеспечения эффективности этого инструмента необходимо задействовать дипломатические и гуманитарные механизмы (Bellamy, 2018). Такой подход предполагает использование правового инструментария иностранных юрисдикций. Например, МУС ввел свою юрисдикцию в Кении и предъявил правительству страны ультиматум о создании специального суда по делам о насилии после выборов (Bellamy, 2018). Юридические меры Международного уголовного суда в данном случае опирались на концепцию R2P, поскольку были направлены на защиту местного населения от насилия. А. Беллами делает вывод о том, что и R2P, и система МУС являются комплексными гуманитарными институтами, призванными предотвратить ППЧ. Несмотря на скептическое отношение к невоенным мерам в рамках R2P, их реализация представляет собой альтернативу военным операциям (Fehl, 2015). Это промежуточная мера, способная предотвратить международные преступления, что делает бесспорным их огромное значение для человечества.

Хотя Международный уголовный суд и R2P совместно играют большую роль в предотвращении преступлений против человечности, использование универсального судебного инструментария должно быть подчинено целям Римского статута (Holvoet & Mema, 2015). Это условие гарантирует эффективность и надежность мер МУС в отношении ППЧ, поскольку обеспечивает судебный надзор за практикой Международного уголовного суда. Таким образом, этот механизм повышает доверие к роли МУС в противодействии преступлениям против человечности и борется

⁸ Application of the Convention on the Prevention and Punishment of the Crime of Genocide (BiH v Serbia and Montenegro), 26 February 2007, ICJ Reports 2007 p. 43, para 166.

⁹ Там же.

с безнаказанностью преступников. Как отмечают исследователи, инструментарий R2P стоит на страже международного правосудия и безопасности, поскольку предусматривает международное вмешательство для обеспечения соблюдения международного права во всем мире (Ercan, 2022).

Подводя итог, можно сказать, что, согласно научным исследованиям и данным судебной практики, концепция R2P основывается на необходимости поддержания мира и безопасности. С этой точки зрения она представляет собой правовую норму, предусматривающую вмешательство в отношении серьезных ППЧ вне установленных юрисдикций. Таким образом, она является адекватным обоснованием для применения иностранных правовых норм, в частности универсальной юрисдикции, в государстве, где совершено преступление. Тем самым преодолеваются рамки суверенитета, которые могут препятствовать защите безопасности человека, что побуждает международное сообщество к выполнению своих обязанностей по защите человечности.

2. Правовые основы для отнесения кибертерроризма к категории «другие бесчеловечные деяния» согласно Римскому статуту

Не вызывает сомнений, что киберпространство устанавливает международные связи между отдельными государствами. В силу технической природы киберпространства террористы используют его преимущества для достижения своих целей. Это позволяет им избегать преследования со стороны национальных правоохранительных органов. Поэтому они действуют на глобальном уровне, угрожая миру во всем мире. Кибертерроризм – это сложившаяся система антигуманной деятельности, пресечение которой требует международно-правовых усилий.

Поддержание всеобщего мира и безопасности является одной из главных целей международных правовых органов, в частности Международного уголовного суда. В силу своих глобальных правовых возможностей он является компетентным органом для преследования международных преступников. Однако в Римском статуте, который его регулирует, говорится исключительно о деяниях, подпадающих под юрисдикцию суда. Кибертерроризм среди них не упоминается. Правда, в нем отмечается, что при определенных условиях юрисдикция суда распространяется и на неупомянутые бесчеловечные деяния¹⁰.

В настоящей статье мы рассмотрим правовые основы, позволяющие расценивать кибертерроризм как преступление против человечности в соответствии с Римским статутом Международного уголовного суда. Степень вреда от этой деятельности достаточна для того, чтобы отнести ее к данной категории, что подводит ее под юрисдикцию МУС. В работе проводится анализ кибертерроризма и обзор литературы с целью выделения его основных элементов. Затем проводится реконцептуализация доктрины международного права о преступлениях против человечности с целью доказать применимость этой концепции к кибертерроризму. Теоретическая значимость исследования состоит в установлении правовых основ для распространения юрисдикции МУС на преследование кибертеррористов. Эта глобальная преступная деятельность требует глобального правового механизма для ее пресечения. Таким образом, международное сообщество сможет бороться с кибертерроризмом, укрепляя мир и безопасность во всем мире.

¹⁰ The Rome Statute of the International Criminal Court (2002), Article 7 (1) (k), A/CONF.183/9.

2.1. Анализ кибертерроризма

В наш информационный век терроризм проник в киберпространство, создав новую угрозу для человечества. Кибертерроризм – это террористическое воздействие на группу лиц с политическими или радикальными целями с использованием Интернета (Broeders et al., 2021). Это особый вид терроризма, который следует анализировать с широкой точки зрения. Кибертеррористы используют возможности Интернета, который сложно контролировать. Французский словарь терминов национальной безопасности характеризует кибертерроризм через фактор риска, связанный с незаконной киберактивностью (Delerue et al., 2019). С помощью Интернета террористические группы могут действовать на транснациональном уровне, преодолевая географические расстояния (Albahar, 2019), поэтому кибертерроризм нужно изучать в международном аспекте. Так, А. Перлофф-Джайлс характеризует кибертеррористов как «врагов человечества» (Perloff-Giles, 2018), проводя параллель между кибертерроризмом и пиратством, поскольку и та и другая деятельность угрожает интересам международной торговли. Исследователь подчеркивает, что в долгосрочной перспективе атаки кибертеррористов ставят под угрозу всю работу сети, что указывает на значительный вред этой деятельности. Кроме того, автор выделяет три признака транснациональных киберпреступлений:

- это преднамеренное действие, причиняющее вред невиновным лицам, например, преднамеренная атака на инфраструктуру страны, правительственные или частные компьютерные системы. Такое действие может быть совершено как государственным, так и негосударственным субъектом. К последней категории и относятся кибертеррористы.

- действие должно происходить в киберпространстве, что позволяет обеспечить анонимность и малозатратность атак,

- действие должно иметь транснациональный характер, поскольку преступники действуют, невзирая на национальные границы. Рассылаемые ими вредоносные программы пересекают границы без паспортов. Кроме того, последствия таких преступлений затрагивают несколько юрисдикций (Perloff-Giles, 2018).

Автор также утверждает, что кибератаки, кто бы их ни совершал, представляют собой незаконное применение силы, что влечет за собой право на самооборону в соответствии со ст. 51 Устава ООН. Это является основанием для применения международного гуманитарного права как релевантной правовой нормы для ликвидации последствий киберконфликтов. Однако для его применения необходимы следующие условия:

- серьезность и масштабность атак. Перлофф-Джайлс считает, что этот параметр должен позволять квалифицировать их как «вооруженное нападение»;

- идентификация исполнителей для установления их ответственности. При этом исследователь признает сложность определения такой идентификации в отношении киберпреступлений (Perloff-Giles, 2018).

Таким образом, исследователь указывает на значение киберпреступлений как уникальной формы агрессии. Эта деятельность, как и обычные вооруженные конфликты, должна приводить к применению международного гуманитарного права. Это означает, что кибертерроризм представляет собой серьезную угрозу человечеству, которая требует использования международных норм.

В книге «Определение международного терроризма» С. Маргарити утверждает, что терроризм угрожает интересам международного сообщества, ущемляя основные права человека, касающиеся всеобщей безопасности и мира (Margariti, 2017). В работе описана глобальная составляющая терроризма и показано, что его последствия выходят за пределы национальных границ и распространяются на все международное сообщество (Margariti, 2017). Поскольку киберпространство не связано с географическими границами государств, все возникающие в нем проблемы приобретают всеобщий характер. Преступные действия в киберпространстве также выходят за пределы границ стран. Следовательно, кибертерроризм неизбежно оказывает влияние на международную безопасность.

В силу отсутствия границ террористические группировки используют киберпространство для достижения своих целей. Известно, что такие организации, как ИГИЛ, используют социальные сети для запугивания путем трансляции видеоконтента. Кроме того, они используют эти сайты в качестве вербовочных площадок. Таким образом, они могут действовать в глобальном масштабе, невзирая на географические границы (Awan, 2017). Эта возможность дает террористам преимущество перед органами правопорядка и безопасности. Поэтому необходимо изучать кибертерроризм как самостоятельный вид преступной деятельности, сочетающий террор и технологии.

Так, В. Коррейя определяет кибертерроризм как «деятельность посредством кибернетических систем, направленную на продвижение политических, социальных или религиозных идеологий против населения, и деятельность, использующую киберсистемы, направленную на угрозу или содействие нанесению ущерба населению, имуществу и/или системам. Кибертерроризм может сочетаться с традиционным терроризмом» (Correia, 2022). Исследователь вводит понятие динамики кибертерроризма, отражающее его изменчивость. Кроме того, она требует ввести особое определение субъективной стороны преступления, которое относится к радикальным мотивам поведения. При этом уточняется, что физическое воздействие не является условием кибертерроризма – возможно нанесение вреда системам, не имеющим физической формы. Предполагается, что введение данного определения будет способствовать международному сотрудничеству в области уголовного преследования и противодействия кибертерроризму. Исследователь также указывает на влияние кибертерроризма на граждан внутри страны. Автор призывает учитывать проблему незаконного использования террористами технологий и изучать данную деятельность на основе комплексного подхода (Correia, 2022).

Напротив, понятие кибертерроризма не включает ненасильственные методы, так как, по определению, он должен приводить к ущербу независимо от его целей. По мнению А. Хеншке и соавторов, использование террористами Интернета для вербовки членов или распространения своих радикальных взглядов само по себе является лишь деятельностью по распространению угроз в адрес целевой аудитории (Henschke, 2021). Отсутствие физического ущерба не позволяет квалифицировать эту деятельность как кибертерроризм. Примечательно, что Хеншке признает, что кибератаки на устройства интернета вещей¹¹ могут привести к физическому воздействию на

¹¹ Интернет вещей – система, позволяющая управлять физическими устройствами посредством кодов искусственного интеллекта.

жертвы (Henschke, 2021). Таким образом, они представляют собой кибертерроризм, поскольку вмешиваются в установленную интернетом вещь связь между информационной сетью и физическим миром. Кроме того, по мнению ученых, в Таллинском руководстве предусмотрено условие, что воздействие кибератаки в физическом мире должно быть ощутимо в той же мере, что и реальное применение силы (Schmitt, 2013). В Руководстве указано, что неразрушительные кибердействия не являются применением силы независимо от их моральных последствий (Schmitt, 2013).

По мнению Д. Бродерс, пока не было зафиксировано кибератак, причинивших физический ущерб (Broeders et al., 2021). Он утверждает, что террористы не обладают необходимыми техническими и финансовыми навыками для совершения кибератак. Кроме того, законодательство Великобритании требует применения насилия для признания акта «террористическим»¹², что исключает ненасильственные действия такого рода. В этой связи К. Стоддарт подчеркивает, что кибертерроризм угрожает инфраструктуре США, поскольку может затронуть деятельность государства. Кроме того, кибертерроризмом можно считать шпионскую деятельность, хотя она может и не носить насильственного характера, что еще раз подчеркивает серьезность проблемы (Stoddart, 2022).

Эти взгляды отражают лишь самый поверхностный анализ кибертерроризма, поскольку не учитывают того факта, что моральные последствия этой деятельности превосходят физический ущерб от нее. Деморализация страны в результате кибертерроризма приводит к опасным экономическим и социальным последствиям. Кибертерроризм порождает гнев среди населения, ставшего объектом нападения, что побуждает его требовать возмездия в виде применения силы (Shandler et al., 2021) и политического ответа, как и в случае обычного терроризма (Shandler et al., 2021). Кроме того, оба вида терроризма мотивируются одними и теми же психологическими стимулами.

По мнению Королевской уголовной прокуратуры (Великобритания), чтобы действия были признаны террористическими, они должны быть мотивированы террором¹³. Аналогичным образом, принятый в Египте Закон о борьбе с терроризмом предусматривает, что даже психологические угрозы невинным людям представляют собой террористический акт, независимо от нанесенного им физического ущерба¹⁴. В соответствии с этим законом, намерение терроризировать гражданское население для реализации целей преступников является достаточным для признания их действий преступными. Таким образом, национальные законодательства отдают приоритет соображениям безопасности, игнорируя условие физического воздействия, которого требует А. Хеншке (Henschke, 2021). Кроме того, в Единой позиции 2001/931/CFSP атаки на национальную инфраструктуру или государственные объекты рассматриваются как террористические акты, в связи с чем к виновным применяются контртеррористические меры¹⁵. Принятая в Австрии Стратегия кибербезопасности

¹² The Terrorism Act 2006, c. 11. <https://clck.ru/34Chci>

¹³ The Crown Prosecution Service. (2021). Terrorism. <https://clck.ru/36kt3Z>

¹⁴ Law No 94/2015, art 2 para 1.

¹⁵ Article 1(3) of Common Position 2001/931/CFSP, см. The EU list of persons, groups and entities subject to specific measures to combat terrorism, Factsheet on 14 January 2015. <https://clck.ru/36kt4j>

для квалификации акта в качестве террористического также требует наличия намерения терроризировать гражданское население с целью нанесения ущерба инфраструктуре или экономике страны¹⁶. Таким образом, в законодательстве многих стран внимание концентрируется на психологическом аспекте терроризма, поскольку именно намерение запугать невинных относит преступное деяние к данной категории. Именно этот отличительный элемент кибертерроризма, который может не причинить физического ущерба, и является определяющим фактором данной категории.

Аналогичным образом С. Маргарити утверждает, что намерение запугать квалифицирует деяние как террористическое, независимо от его мотивов (Margariti, 2017). Этот элемент отличает терроризм от обычных преступлений. Это та специфическая субъективная сторона преступления, которая определяет его классификацию. Исследователь принимает этот стандарт в качестве всеобщего детерминанта объективной стороны международного терроризма, необходимого для применения к нему универсальных правовых норм (Margariti, 2017).

Таким образом, необязательность физического воздействия для признания акта террористическим усиливает инклюзивную тематику исследований кибертерроризма, что согласуется с определением В. Коррейя, рассмотренным выше (Correia, 2022). Даже имея только моральные последствия, кибертерроризм угрожает всеобщему миру и безопасности, так как может привести к вооруженному конфликту. В отличие от обычного терроризма люди не могут укрыться от кибертерроризма; коды, которые используют кибертеррористы для нанесения ущерба вычислительным системам целевой аудитории, проникают через многочисленные уровни защиты. Таким образом, отсутствие кибербезопасности дестабилизирует мир и безопасность во всем мире. Кибертерроризм может быть возведен в ранг врага человечества, как это предлагает А. Перлофф-Джайлс (Perloff-Giles, 2018).

2.2. Контекстуальные элементы преступлений против человечности: другие бесчеловечные деяния

Статья 7(1)(к) Римского статута включает термин «другие бесчеловечные деяния» для установления юрисдикции МУС в отношении этих тяжких деяний. Этот термин прочно вошел как в доктрину, так и в судебную практику. Однако для целей настоящей работы мы рассмотрим элементы этого понятия, чтобы сравнить их и доказать его применимость к кибертерроризму как международной противоправной деятельности. Поскольку данный термин был сформулирован в рамках международного права, необходимо изучить его элементы с точки зрения международной доктрины и судебной практики.

Изначально ст. 7(1)(к) Статута устанавливает, что категория «другие бесчеловечные деяния» является неотъемлемой частью ППЧ, запрещенных Статутом (Broeders et al., 2021). В статье перечислены следующие элементы этого деяния, аналогичные основным элементам преступлений против человечности: бесчеловечные действия, намерения причинить психологические или физические страдания. Однако данное определение шире, чем определение ППЧ, чтобы дать возможность преследовать деяния, не включенные в преступления против человечности.

¹⁶ Federal Chancellery of the Republic of Austria. (2013). Austrian Cyber Security Strategy. Vienna. <https://clck.ru/36kt6E>

В работе Р. Атаджанова утверждается, что системный характер преступлений против человечности отличает их от обычного преступного поведения (Atadjanov, 2019). Таким образом, организованность поведения отражает элемент контекста, необходимый для квалификации деяния в качестве преступления против человечности. Именно эта организованность позволила Гоббсу утверждать, что ППЧ выражают «крайнюю степень зла» (Hobbs, 2017). Таким образом, этот элемент отражает их масштабность и тяжесть для законных интересов человечества. Однако, по мнению Сеада Хусейн Адема, понятие ППЧ страдает от нормативного пробела в международной доктрине, который Статут стремится восполнить путем перечисления элементов, квалифицирующих деяние как преступление против человечности (Adem, 2019). Исследователь приходит к выводу, что судебная практика по делам о преступлениях против человечности также помогает устранить этот пробел, поскольку специальные трибуналы и Международный уголовный суд разработали инклюзивный подход, который разрешил эту дилемму (Adem, 2019).

Комиссия по международному праву (далее – КМП) требует, чтобы подобные деяния и их последствия рассматривались как ППЧ¹⁷. Кроме того, утверждается, что они могут быть совершены негосударственными субъектами¹⁸. Поэтому КМП допускает классификацию деяний, совершенных группами или организациями, в качестве ППЧ в соответствии с положениями Римского статута. По мнению Комиссии, преступления против человечности могут совершаться не только государствами, но и независимыми структурами или отдельными лицами. Кроме того, основным элементом данного преступления КМП считает многочисленность жертв. Это условие не позволяет отнести отдельные ограниченные деяния к данной категории.

Что касается судебной практики, то термин «бесчеловечные деяния» отражает развитие классификации преступлений против человечности. Этот подход использовался в 18 делах, рассмотренных МУС, в качестве альтернативного ответа на правовой вакуум (MacNeil, 2021). В деле Prosecutor v Jean-Pierre Bemba Gombo¹⁹ утверждается, что преступления против человечности имеют четыре составляющих: нацеленность на гражданских лиц, масштабность, совершенные действия, субъективную сторону²⁰. Кроме того, Международный уголовный суд считает преступлениями против человечности бесчеловечные действия, причиняющие психологический ущерб²¹. В деле Prosecutor v Germain Katanga и Mathieu Ngudjolo Chui²² суд постановил, что серьезные нарушения основных прав человека, закрепленных в международном праве, являются бесчеловечными деяниями в соответствии со ст. 7(1)(k) Статута²³.

¹⁷ The International Law Commission, Draft Code of Crimes against the Peace and Security of Mankind, 1996 UN Doc. A/51/10 article 18 (k), c. 47. <https://clck.ru/36kt7d>

¹⁸ Там же.

¹⁹ Case No. ICC-01/05-01/08.

²⁰ Там же, para 117 и (Park & Switzer, 2020).

²¹ Там же. Также см. International Criminal Court. (2013). Elements of Crimes. ISBN 92-9227-232-2, ICC-PIOS-LT-03-002/15_Eng. <https://clck.ru/36ktC8>

²² Case No. ICC-01/04-01/07.

²³ Там же, para 448. МУС применил тот же принцип в запросе The Request for authorization of an investigation pursuant to article 15 относительно ситуации в Бангладеш и Республике Союза Мьянма, Case No. ICC-01/19, para 128.

Как отмечает Дж. Куигли, по классификации МУС контекстуальными элементами категории «другие бесчеловечные деяния» является преднамеренное причинение сильных страданий или психологического или физического вреда (Quigley, 2023). По мнению ученого, это самостоятельная категория уголовного права, не требующая установления связи с другими включенными преступлениями (Quigley, 2023).

Международным уголовным трибуналом по бывшей Югославии (далее – МТБЮ) было принято решение, что действия, ущемляющие человеческое достоинство, являются «бесчеловечными деяниями» в соответствии с Римским Статутом²⁴. Таким образом, Трибунал расширяет толкование этого термина, выходя за рамки Статута и охватывая новые преступные деяния. Такое мнение Трибунала является результатом доктринального вакуума в отношении определения «бесчеловечных деяний». Кроме того, МТБЮ устанавливает элементы, по которым деяние может быть признано бесчеловечным:

- тяжесть совершенных деяний;
- психологический или физический вред или ущерб человеческому достоинству;
- субъективная сторона²⁵.

В деле *Prosecutor v Milorad Krnojelac*²⁶ бесчеловечные деяния также определяются как преднамеренные действия, наносящие серьезный психологический или физический ущерб невиновным лицам²⁷. Эта императивная норма квалифицирует действия преступников как преступления против человечности в силу тяжести их последствий. Европейский суд по правам человека в делах *Liu v Poland*²⁸ и *M. T. and Others v. Sweden*²⁹ использует термин «бесчеловечный» для обозначения действий, унижающих достоинство человека и нарушающих его основные права.

Таким образом, международная судебная практика устанавливает, что эти действия относятся к категории ППЧ, а именно к категории «другие бесчеловечные деяния». Данный термин принят в качестве условия в целях расширения юрисдикции в отношении преследования преступлений против человечности для обеспечения эффективной защиты. Таким образом, Римский статут отражает гибкую судебную практику, позволяющую использовать расширенную юридическую терминологию для контекстуализации не включенных в него злодеяний.

2.3. Применимость категории «другие бесчеловечные деяния» к кибертерроризму

В литературе, посвященной контекстуальным элементам термина «другие бесчеловечные деяния», подчеркивается их тяжесть; эксперты исходят из того, что такие деяния наносят ущерб психологическому и физическому благополучию невинных людей. Анализ этих элементов отражает крайнюю тяжесть этих деяний. Таким

²⁴ *Prosecutor v Mucić et al*, Trial judgment, 16 November 1998, IT-96-21-T, (Celebici, Trial judgment), paras 521–522.

²⁵ *Prosecutor v Karadžić*, Trial judgment, 24 March 2016, IT-95-5/18-T, (Karadžić, Trial judgment), para 494.

²⁶ IT-97-25-T.

²⁷ Там же, прим. 382.

²⁸ Application no. 37610/18, on 6 October 2022.

²⁹ Application no. 22105/18, on 20 October 2022.

образом, другие действия, выражающие такие же злодеяния, должны быть также классифицированы как «другие бесчеловечные деяния», если в них присутствуют те же контекстуальные элементы. Иначе говоря, определяющим фактором такой классификации деяния является применимость к нему этих элементов.

Прежде всего, кибертерроризм нарушает основные принципы международного гуманитарного права (Werle & Jeßberger, 2014). Во-первых, он нарушает минимальные стандарты человечности, распространяя угрозы. Во-вторых, причиняемый им ущерб гражданскому населению выходит за рамки стандартов соразмерности, поскольку преступный умысел террористов относится ко всем людям. Кибертеррористы ставят во главу угла достижение своих целей, невзирая на страдания невинных гражданских лиц. Этот недискриминационный характер кибертерроризма согласуется с интерпретацией преступлений против человечности Римским статутом³⁰. Согласно Статуту, для признания преступления принадлежащим этой категории необходимо, чтобы деяние было совершено против гражданского населения. В международном праве общепризнано, что ущерб от этих преступлений может являться как физическим, так и психологическим. Даже простое пренебрежение человеческим достоинством значительно усугубляет выдвинутые обвинения³¹.

В работе С. Маргарити жертвой кибертерроризма выступает все международное сообщество, поскольку он направлен против всеобщего мира и безопасности (Margariti, 2017). Кроме того, общим для кибертерроризма и преступлений против человечности является систематический характер преступлений против человечности, на который указывает Гоббс (Hobbs, 2017). Также оба этих вида преступлений имеют транснациональные последствия, что дает основания для международного вмешательства. Они представляют собой угрозу человечеству, что позволяет отнести их к одной категории. Кроме того, как указывает Р. Атаджанов, элемент систематичности применим к кибертерроризму, поскольку он угрожает всеобщему миру и безопасности и представляет собой широкомасштабное организованное нападение на гражданское население (Atadjanov, 2019). Кибертерроризм причиняет серьезный вред международному сообществу, поскольку его участники ставят под угрозу основные права человека. Их систематические действия нарушают «мирное сосуществование» (Atadjanov, 2019) целевых групп и принципы человечности, предусмотренные Всеобщей декларацией прав человека 1948 г.³² Кроме того, к кибертерроризму применим такой контекстуальный элемент, как систематический характер ППЧ, поскольку он угрожает всеобщему миру и безопасности и представляет собой широкомасштабное недискриминационное организованное нападение на гражданское население.

Данное мнение подтверждает и обсуждаемое в литературе утверждение о том, что кибертерроризм, причиняющий нефизический ущерб, является преступлением против человечности. Такие деяния направлены на гражданское население в целом, без каких-либо различий, и преступники намеренно игнорируют жертвы среди гражданского населения при достижении своих целей. Более того, Комиссия по международному праву в проекте Конвенции о предупреждении и наказании преступлений

³⁰ The Rome Statute, Art 7.

³¹ Prosecutor v Karadžić, Trial judgment, 24 March 2016, IT-95-5/18-T, (Karadžić, Trial judgment), para 494.

³² The Universal Declaration of Human Rights, the United Nations, GA-Res 217/1948. <https://clck.ru/36ktDK>

против человечности считает психологический ущерб достаточным для квалификации деяния в качестве преступления против человечности³³. Таким образом, в доктрине международного права физический ущерб не является основным условием совершения преступлений против человечности. Аналогичным образом, международная судебная практика устанавливает, что душевные страдания достаточны для квалификации действий преступников в качестве преступлений против человечности в соответствии со ст. 7 (1) (k) Статута. Такой подход подчеркивает серьезность психологического ущерба, наносимого кибертерроризмом.

При этом ряд ученых не требует наличия оговорки о недискриминационном характере деяния для квалификации его в качестве преступления против человечности (Maguir, 2022). Так, Р. Магауйр утверждает, что они должны носить систематический характер в отношении групп гражданского населения с осознанием преднамеренности действий исполнителей. Аналогичным образом Апелляционной палатой Специального трибунала ООН по Ливану было указано, что субъективной стороной таких деяний должно быть намерение распространить террор с помощью средств, представляющих опасность для гражданского населения³⁴. Также было отмечено, что обычное международное право не ограничивает терроризм определенными средствами. Таким образом, признается, что террористы могут использовать кибернетические средства для достижения своих целей. Определяющим фактором является намерение осуществить публичный террор, независимо от формы преступного поведения.

Кроме того, Цилонис отмечает, что понятие «организационная политика», предусмотренное ст. 7 (2)(a) Римского статута, распространяется и на негосударственных субъектов, например, террористов (Tsilonis, 2019). Террористическая деятельность может не поддерживаться государством, чтобы МУС имел право преследовать ее исполнителей. Цель этого положения – усилить защиту человечества от тяжких преступлений. Правовые цели ст. 7 выходят за рамки буквального толкования указанного термина и подразумевают террористическое поведение.

Указанные элементы бесчеловечных деяний совпадают с определением кибертерроризма, которое предлагает В. Коррейя (Correia, 2022). Как в практике, так и в доктрине международного права установлено, что преднамеренные тяжкие деяния, направленные против невиновных гражданских лиц и наносящие ущерб их основным правам, являются, независимо от их формы, бесчеловечными деяниями в соответствии со ст. 7 Римского статута. Очевидно, что это определение можно применить и к кибертерроризму. Нанося удары по инфраструктуре страны, кибертеррористы затрагивают гражданское население. Кроме того, широкомасштабные атаки необходимы преступникам для устрашения общества, что является отличительной чертой их деятельности. Далее, кибертеррористы всегда действуют против всего гражданского населения, а не отдельных его групп. Наконец, для достижения своих целей преступники должны терроризировать невинных людей. Анализ элементов киберпреступлений, приведенный в работе А. Перлофф-Джайлс (Perloff-Giles, 2018), согласуется с содержанием императивных норм, установленных международными судами. Сюда относятся, в частности, примеры бесчеловечных

³³ The International Law Commission, “Report of the International Law Commission”, Seventy-first session (29 April – 7 June and 8 July – 9 August 2019) A/74/10, c. 12. <https://clck.ru/36ktFT>

³⁴ The UN Special Tribunal of Lebanon Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, 16 February 2011, Case No. STL-11-01/1 (STL Decision).

деяний в нарушение прав человека, приведенные в Европейской конвенции по правам человека. Действительно, кибертерроризм изобилует примерами деяний, унижающих человеческое достоинство.

В заключение следует отметить, что ученые и юристы-практики развивают доктрину кибертерроризма как преступления против человечности в соответствии с Римским статутом. Кибертеррористы систематически находят новых жертв, не считаясь с серьезными последствиями. Транснациональный характер таких преступлений дает основания для борьбы с ними на международном уровне. Независимо от используемых методов, состояние страха, которое навязывают преступники, уже само по себе является достаточным основанием для того, чтобы считать кибертерроризм преступлением против человечности. Кроме того, распространение юрисдикции Международного уголовного суда на преследование кибертеррористов позволяет квалифицировать их действия как преступления против человечности. Категория бесчеловечных деяний, предусмотренная ст. 7 (1) (k) Римского статута, должна включать в себя кибертерроризм. Этот вывод предполагает использование универсальных правовых механизмов, находящихся под юрисдикцией МУС, для преследования кибертеррористов. Таким образом, кибертеррористы попадут под юрисдикцию МУС, как и в случае с другими лицами, совершившими преступления против человечности.

3. Универсальная юрисдикция для преследования ППЧ

Развитие международного сотрудничества в судебной сфере привело к возникновению универсального принципа юрисдикции. Этот принцип предполагает возможность преследовать и судить преступников независимо от их местонахождения или гражданства. Он направлен на достижение правосудия на международном уровне, требуя выхода за рамки традиционных юрисдикций для пресечения тяжких преступлений. В работе Блешич (Blešić, 2022) применение универсальной юрисдикции ограничено международными преступлениями, поскольку они налагают всеобщее обязательство преследовать виновных.

Концепция универсальной юрисдикции представляет собой значительное достижение в международном уголовном праве, поскольку она позволяет государствам и соответствующим органам осуществлять преследование международных преступников на глобальном уровне, независимо от их гражданства (Mung'omba, 2022). Таким образом, универсальная юрисдикция ограничивает их возможности избежать наказания, способствуя укреплению международного уголовного правосудия. Она представляет собой право международного сообщества вмешиваться везде, где совершены ППЧ, с целью наказать преступников (Mung'omba, 2022). Примечательно, что, по мнению исследователя, универсальная юрисдикция не требует прямой связи между судебным органом, осуществляющим преследование, и преступлением (Mung'omba, 2022). Универсальная юрисдикция, по его мнению, отличается от основных норм в этой области, что соответствует ее предназначению в обеспечении международного уголовного правосудия (Mung'omba, 2022)³⁵. Это отличие обусловлено необходимостью обеспечить

³⁵ При этом было вынесено решение, что преступник должен лично присутствовать в суде согласно принципам Принстона. См. также Global Policy Forum. (2021, June 2). Princeton Principles on Universal Jurisdiction: Princeton Project on Universal Jurisdiction. <https://clck.ru/36ktLY>

правосудие и сдерживание в отношении ППЧ (Mung'omba, 2022). Таким образом, универсальная юрисдикция оформлена в международном праве как уникальное средство преследования и сдерживания преступлений против человечности. На уровне ООН делегации государств на 73-й юридической сессии приняли решение, что универсальная юрисдикция представляет собой эффективный инструмент для преследования основных видов преступлений, в том числе и ППЧ³⁶.

Можно утверждать, что государства устанавливают национальную юрисдикцию как на субъективной, так и на объективной основе (Kittichaisaree, 2017). Международная судебная практика ограничивает национальную юрисдикцию традиционными факторами³⁷, тем более что не существует конвенции, устанавливающей нормы универсальной юрисдикции. Более того, суды различных стран должны применять свою «презумптивную юрисдикцию» в отношении преступлений против человечности. Как утверждает Магуайр, интересы жертв оправдывают приоритет национального преследования за эти преступления (Maguir, 2022). Однако другие исследователи критикуют такой подход, считая, что он приведет к злоупотреблению властью со стороны отдельных государств и лишит обвиняемого права на справедливое судебное разбирательство (Soler, 2019). Таким образом, применение универсальной юрисдикции в отношении ППЧ должно быть справедливым и пропорциональным, чтобы гарантировать эффективное правосудие (Soler, 2019). Эти условия поддерживают баланс между противодействием преступлениям против человечности и уважением национального суверенитета. Также этот ученый призывает выработать единый подход к отказам от принципа *aut dedere aut judicare*, чтобы покончить с безнаказанностью лиц, совершивших ППЧ, которая считается основной причиной того, что такие преступления продолжаются (Maguir, 2022). Таким образом, надлежащее применение универсальной юрисдикции способствует укреплению международного уголовного правосудия, поскольку расширяет юрисдикционные инструменты для преследования и экстрадиции лиц, совершивших ППЧ. Кроме того, такое применение способствует выполнению государствами своих обязательств по преследованию основных преступлений, тем самым они защищают права человека и укрепляют традиционное понимание принципов правопорядка (Maguir, 2022). Примечательно, что Солер отстаивает право третьих государств на преследование лиц, совершивших преступления против человечности, утверждая, что универсальная юрисдикция восполняет отсутствие территориальной юрисдикции и юрисдикции на основе гражданства (Maguir, 2022). Универсальная юрисдикция, таким образом, не противоречит обязанности государства преследовать указанные преступления (Maguir, 2022).

Хотя принцип универсальной юрисдикции ограничивает безнаказанность преступников, она может рассматриваться и как угроза национальному суверенитету и стабильности³⁸. Так, Африканский союз отклонил испанский ордер на арест генерал-лейтенанта Эммануэля Каренци Караке, посчитав его нарушением международного права и злоупотреблением принципом универсальной юрисдикции. Союз также осудил попытки

³⁶ The 6th Committee of the UN General Assembly – Legal (73rd Session), 'The scope and application of the principle of universal jurisdiction (Agenda item 87)', См. resolution 72/120. <https://clck.ru/36ktQV>

³⁷ См. the Lotus Case (France v. Turkey), Judgment of 7 Sept. 1927, Series A No. 10.

³⁸ African Union Doc PSC.PR/COMM.(DXIX) Communiqué, Peace and Security Council 519th, 26 June 2015, paras 4-5. <https://clck.ru/36ktSW>

европейских судов подчинить себе судебные органы африканских стран путем злоупотребления универсальной юрисдикцией³⁹. Эти факты отражают противоречивость принципа универсальной юрисдикции. Данный механизм позволяет преследовать за преступления против человечности и положить конец безнаказанности преступников, их совершающих, однако его применение не лишено недостатков. В работе Ньяво это обосновывается отсутствием международного соглашения или иного документа, определяющего универсальную юрисдикцию и объясняющего ее применение (Nyawo, 2023). Ученый утверждает, что универсальная юрисдикция необходима для противодействия ППЧ, поскольку в этом заинтересованы все государства (Nyawo, 2023). Кроме того, он обосновывает необходимость использования универсальной юрисдикции всеобщим моральным долгом, который постулируется в теории естественных прав (Nyawo, 2023). Этот долг обязывает международное сообщество сотрудничать в борьбе со злодеяниями, угрожающими миру и безопасности на планете.

Совет безопасности ООН также говорит об обязанности преследовать преступления против человечности и наказывать виновных, независимо от их гражданства⁴⁰. Данная резолюция отражает понимание ППЧ как особо тяжких преступлений, подразумевающая единую модель преследования виновных.

Представитель организации Human Rights Watch Лотте Лейхт утверждает, что ООН разработала механизм судебного преследования лиц, совершивших ППЧ. Этот механизм предусматривает работу постоянного прокурора, который инициирует расследование случаев преступлений против человечности, не создавая специального суда. Его юрисдикция распространяется повсеместно, независимо от судебных или политических барьеров⁴¹.

3.1. Принцип *aut dedere aut judicare* в отношении кибертерроризма

Аксиомой международного права является положение о том, что обвинения в терроризме предполагают применение универсальной юрисдикции в силу их тяжести (Soler, 2019). Поскольку принцип *aut dedere aut judicare* представляет собой общий принцип международного права, международное сообщество должно использовать его для борьбы с кибертерроризмом. Тяжесть этого преступления, недостаточность защиты прав человека на международном уровне, а также угроза миру вследствие безнаказанности кибертеррористов – все это свидетельствует в пользу применения универсальной юрисдикции как международными, так и национальными судами с целью преследования и выдачи преступников. Только таким образом может быть обеспечено сдерживание кибертерроризма на глобальном уровне.

Характеризуя киберпреступников как врагов человечества, А. Перлофф-Джайлс (Perloff-Giles, 2018) поддерживает введение универсальной юрисдикции для преследования и выдачи кибертеррористов. Она также утверждает, что в соответствии с Конвенцией ООН по морскому праву (UNCLOS) государства могут преследовать пиратов, где бы они ни действовали, в том числе «вне территориальных вод», т. е. вне

³⁹ Там же, пара 6.

⁴⁰ UNSC/S/RES/138, 23 June 1960, para 4. <https://clck.ru/36ktdL>

⁴¹ The European Parliament. (2018, June 28). Workshop: Universal jurisdiction and international crimes: Constraints and best practices. Brussels, EP/EXPO/B/COMMITTEE/FWC/2013-08/Lot8/21.

пределов национальной юрисдикции⁴². Затем исследователь расширяет понятие «вне территориальных вод», включая в него киберпространство, поскольку считает его транснациональной сферой взаимодействия (Perloff-Giles, 2018). Свою точку зрения она обосновывает решением американского суда, постановившего, что нахождение «вне территориальных вод» не является условием для применения универсальной юрисдикции в отношении пиратства⁴³. Сравнивая пиратство и киберпреступность, ученый показывает, что и то и другое угрожает международной торговле, поскольку кибератаки могут нарушить работу сайтов коммерческих и финансовых служб. Таким образом, принцип универсальной юрисдикции является эффективным подходом к пресечению транснациональных киберпреступлений.

Применение принципа универсальной юрисдикции осложняют технические вопросы, например, облачные вычисления, поскольку в киберпространстве сразу несколько государств могут заявить о своей экстерриториальной юрисдикции в отношении облачной деятельности, как было показано в работе (Kittichaisaree, 2017). Рассматривая международно-правовые документы, ученый упоминает, что разрешение на экстерриториальное преследование «несанкционированной трансляции сигнала» с судна, находящегося вне территориальных вод⁴⁴, распространяется и на передачу сигналов кибернетическими средствами (Kittichaisaree, 2017). Таким образом, он применяет термин «вещание» к интернет-сайтам, таким как Facebook⁴⁵ и Twitter⁴⁶. Эти онлайн-платформы используются террористами для трансляции своей идеологии и вербовки, что дает основания государствам применять свою юрисдикцию. Кроме того, Конвенция 1973 г. о предотвращении и наказании за преступления против лиц, пользующихся международной защитой, устанавливает универсальную юрисдикцию в отношении преступных деяний, которая распространяется и на кибертерроризм, если они направлены против лиц, указанных в ст. 1⁴⁷. Это требует от государств-участников использовать свои правовые инструменты для пресечения этой деятельности, в соответствии с целями Конвенции. В связи с быстрым развитием средств доступа в Интернет затраты на организацию кибертеррористической деятельности очень малы по сравнению с ее последствиями (Kittichaisaree, 2017). Поэтому необходимо расширить область применения Будапештской конвенции о киберпреступности и создать глобальную сеть для преследования кибертеррористов.

Как утверждает Магуайр, преследование кибертерроризма в рамках национальных судебных систем оказывается эффективным, поскольку оно мотивировано доверием пострадавших к этим системам⁴⁸. Кроме того, презумптивная юрисдикция отражает в своей основе применение к этим преступлениям универсальной юрисдикции;

⁴² Article 101 c of the United Nations Convention on the Law of the Sea, 1833 U.N.T.S. 397 (entered into force Nov. 16, 1994).

⁴³ United States v. Ali, 718 F.3d 929, 935-38 (D.C. Cir. 2013).

⁴⁴ Art 109, the UNCLOS.

⁴⁵ Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

⁴⁶ Социальная сеть заблокирована на территории Российской Федерации за распространение незаконной информации.

⁴⁷ Art 3 of the 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, entered into force on 20 February 1977.

⁴⁸ См. the Lotus Case (France v. Turkey), Judgment of 7 Sept. 1927, Series A No. 10.

тем самым обеспечивается защита пострадавших от юрисдикционной уязвимости, связанной с преследованием кибертерроризма (Kittichaisaree, 2017). Следовательно, такой подход соответствует принципу экстерриториального наказания киберпреступников, независимо от их местонахождения или гражданства. При этом последствия кибертерроризма могут затрагивать несколько юрисдикций, что приводит к их конфликту. Таким образом, принцип взаимодополняемости МУС сохраняет свое значение для устранения недостатков государственных органов в преследовании кибертеррористов. Однако эта система обратной комплементарности отражает вертикальную иерархию между Международным уголовным судом и его членами в вопросе преследования основных преступлений (Burens, 2016). Так, Лаура Буренс утверждает, что горизонтальный межгосударственный механизм взаимодополняемости усиливает принцип универсальной юрисдикции в соответствии с Римским статутом. Кроме того, ее подход включает государство, в котором находится преступник, в качестве обязательного условия для использования универсальной юрисдикции в процессе уголовного преследования (Burens, 2016). Такая интеграция вертикальной и горизонтальной взаимодополняемости устраняет проблемы применения универсальной юрисдикции благодаря прозрачности принципа субсидиарности (Burens, 2016)⁴⁹. Кроме того, в Резолюции 72/120 отмечается, что использование принципа универсальной юрисдикции должно подчиняться действию международного права и принципу субсидиарности, чтобы предотвратить злоупотребления или неэффективное использование данного принципа⁵⁰. Солер, в свою очередь, утверждает, что такая интеграция необходима для адекватного применения универсальной юрисдикции, чтобы преодолеть недостаточность принципа субсидиарности (Soler, 2019).

Что касается национальных законов, то законодательство Великобритании расширяет свою юрисдикцию на террористические преступления, независимо от их объективной стороны, в соответствии с целями, указанными в ст. 63B⁵¹. Такая экстерриториальная юрисдикция способствует защите от кибертерроризма: Королевская уголовная прокуратура может использовать свои правовые инструменты для экстерриториального преследования преступников⁵², если указанная статья содержит указания на их субъективную сторону. Кроме того, судебные органы Великобритании в деле *R v. Kumar Lama*⁵³ указали, что национальный суд должен использовать универсальную юрисдикцию для преследования тяжких преступлений. При этом стоит отметить, что данный процесс подвергся критике из-за недостатков сбора доказательств за рубежом, которые привели к тому, что суд признал полковника Ламу невиновным⁵⁴. Аналогичным образом Закон о борьбе с преступлениями в сфере информационных

⁴⁹ Л. Буренс утверждает, что данный принцип служит поддержанию баланса между суверенитетом государств и необходимостью преследовать международных преступников.

⁵⁰ Resolution 72/120, Supra 17.

⁵¹ Terrorism Act 2000, the UK, 63A- 63D.

⁵² The Crown Prosecution Service (2021), 'Jurisdiction', (CPS: Legal Guidance on 26 July 2021). <https://clck.ru/36ktjD>

⁵³ Case no. 2013/05698 (Central Criminal Court, London, 2016).

⁵⁴ Hovell, D. (2017, April 6). The 'Mistrial' of Kumar Lama: Problematizing Universal Jurisdiction. EJIL Talk – Blog of the European Journal of International Law. <https://clck.ru/36ktkR>

технологий⁵⁵ расширил юрисдикцию Египта в отношении киберпреступлений, включив в нее преступления, совершенные негражданами при следующих условиях⁵⁶:

– Преступление было совершено на борту любого морского, воздушного или наземного транспорта, зарегистрированного в Египте или функционирующего под его флагом.

– Жертвой является гражданин Египта.

– Преступление планировалось, отслеживалось или финансировалось в Египте.

– Преступление совершено организованной группой, действовавшей в нескольких странах, в том числе и в Египте.

– Преступление может нанести ущерб интересам или безопасности Египта, а также интересам или безопасности любого гражданина или жителя страны.

– Преступник был обнаружен в Египте после совершения преступления и еще не был экстрадирован.

Такой широкий подход египетского законодателя является следствием правового вакуума, в котором оказались египетские судьи в отношении кибертерроризма. Он также демонстрирует комплексный взгляд на применение универсальной юрисдикции в киберпространстве для усиления правовой защиты от кибертерроризма.

В заключение следует отметить, что транснациональный характер кибертерроризма, а также его серьезное влияние на всеобщий мир и безопасность подталкивают международное сообщество к принятию универсальной юрисдикции для преследования и наказания виновных. Этот подход является адекватным механизмом для противостояния киберпреступникам, поскольку согласуется с обязанностями государства по преследованию основных преступлений, признанными в международном праве. Действительно, безнаказанность кибертеррористов ведет к росту числа их преступлений. Поэтому международное сообщество должно объединить свои правовые усилия для выработки единого глобального понимания принципа универсальной юрисдикции, чтобы избежать правового вакуума.

4. Заполнение пробела в законодательстве

Общепризнано, что кибертерроризм является одним из основных видов противоправной деятельности в киберпространстве в силу возможностей последнего. Широкий охват, распространяющийся и на реальный мир, позволяет преступникам эффективно достигать своих целей. Таким образом, складывается глобальная тема кибертерроризма, для противостояния которому необходимо использовать международно-правовые механизмы. Однако глобальный характер этих механизмов может превратить их в инструменты вмешательства во внутренние дела независимых государств. Проще говоря, государства могут выступать против использования этих механизмов, обосновывая это соображениями суверенитета. Возникает дилемма в отношении преследования и суда над кибертеррористами, что усиливает их безнаказанность в реальной международно-правовой практике. Таким образом, они угрожают миру и безопасности на планете. Чтобы преодолеть противодействие государств и убедить их в необходимости сотрудничества в борьбе с кибертерроризмом как

⁵⁵ Law No 175/2018.

⁵⁶ Там же, pt 1 art 3.

международной опасностью, эти глобальные механизмы должны иметь прочную правовую основу.

4.1. Объяснение существующей дилеммы

Несмотря на стабильность международно-правовых норм, их применение еще не стало чем-то само собой разумеющимся. Различные интересы государств и интерпретация ими международно-правовых концепций затрудняют создание единого порядка применения международных императивных норм. Возвращаясь к теме исследования, международно-правовая практика показывает, что обе нормы международного права – принципы R2P и универсальной юрисдикции – постоянно подвергаются сомнению. Скептиками выступают либо юристы, либо дипломаты, поскольку отсутствует единство в понимании этих концепций. Таким образом, попытка закрепить принцип универсальной юрисдикции на основе концепции R2P принесет результат только в том случае, если позиция ее критиков также будет тщательно изучена, а ее траектория контекстуализирована.

Международно-правовая практика показывает, что применение универсальной юрисдикции для противодействия кибертерроризму еще не стало приемлемым механизмом. Многие государства и даже международные организации выступают против него и препятствуют осуществлению правовых мер, основанных на принципе универсальной юрисдикции. Такое противодействие, очевидно, проявилось и в заявлении Африканского союза, где говорилось, что универсальная юрисдикция нарушает стабильность всего континента⁵⁷. Хотя принятые европейским судом меры касались ППЧ в Руанде, они были восприняты в чисто политическом контексте, связанном с воспоминаниями о европейской колонизации Африки. Подобные взгляды усиливают безнаказанность преступников и препятствуют осуществлению правосудия.

Кроме того, дискуссии на 12-м заседании Шестого комитета Генеральной Ассамблеи ООН обнаружили существенный пробел в отношении универсальной юрисдикции. В то время как Германия представила опыт судебного преследования официальных лиц Сирии в национальном суде за совершение преступлений против человечности⁵⁸, Колумбия заявила, что применение универсальной юрисдикции должно осуществляться на основании двустороннего или международного договора⁵⁹. Большинство представителей отметили, что для эффективности универсальной юрисдикции необходимо ее включение в национальные правовые системы⁶⁰. Тем самым прослеживается различие в отношении государств к универсальной юрисдикции, что углубляет разрыв в ее концептуализации и применении. Кроме того, государства могут выступать против универсальной юрисдикции, поскольку не желают разрешать иностранной юрисдикции преследовать кибертеррориста на своей территории и выдавать его иностранной юрисдикции. Так, Блешич утверждает,

⁵⁷ African Union Doc PSC.PR/COMM.(DXIX) Communiqué, Peace and Security Council 519th, 26 June 2015, paras 4-5. <https://clck.ru/36ktSW>

⁵⁸ Speakers Disagree on How, When, Where Universal Jurisdiction Should Be Engaged, as Sixth Committee Takes up Report on Principle. (2022, October 12). UN Press. <https://clck.ru/36ktp8>

⁵⁹ Там же, para 7.

⁶⁰ Там же, paras 3, 4, 5 & 8.

что определяющим фактором применения универсальной юрисдикции является политическая воля (Blešić, 2022). Она, в свою очередь, зависит от наличия двусторонних договоров между государствами.

Более того, децентрализация международного уголовного правосудия приводит к тому, что универсальная юрисдикция зависит только от воли и действий государств (Nyawo, 2023). Это существенный недостаток, поскольку может привести к политическим конфликтам между государствами, особенно в условиях отсутствия всеобщих правил в отношении универсальной юрисдикции. Разработка международно-правовых норм является необходимым условием стабилизации судебного статуса в отношении уголовного преследования за совершение преступлений против человечности. Таким образом, для преодоления этого барьера универсальная юрисдикция нуждается в универсальном обосновании, соответствующем ее целям и природе.

В международной доктрине отмечается, что концепция R2P имеет ряд недостатков. По словам Ройер, практика международного права показывает, что государства могут рассматривать принцип R2P как отражение западного империализма (Royer, 2021). Он утверждает, что этому мнению способствует использование данной концепции для оправдания военных интервенций в случае совершения ППЧ (Royer, 2021). Кроме того, концепция R2P угрожает равновесию при поддержании правопорядка (Royer, 2021), что приводит к хаосу внутри государства. Эта дихотомия лежит в основе критики R2P (Royer, 2021). Поэтому ученый предлагает юристам обратить особое внимание на этот аспект данной концепции, чтобы гарантировать беспристрастность его применения (Royer, 2021). Далее он утверждает, что доктрина должна оценивать вмешательство в рамках концепции R2P отдельно по каждому случаю (Royer, 2021), чтобы избежать несправедливости в международно-правовой практике (Royer, 2021). Обобщение суждений о R2P ставит под угрозу доверие к этой гуманитарной концепции, а злоупотребление ею ни в коем случае не должно приводить к отказу от нее. Поэтому определяющим фактором применения R2P являются обстоятельства каждого конкретного дела. Такой механизм отделяет этот принцип от политической воли государств и способствует его беспристрастному применению. Наконец, по мнению Ройер, критиковать концепцию R2P могут лишь те, кто неспособен оценить последствия зла, которому она противостоит.

Таким образом, необходимость применения принципа универсальной юрисдикции против кибертерроризма перевешивает доводы, объясняющие противодействие государств. Кибертерроризм как глобальное преступное деяние требует использования международного инструментария, выходящего за рамки внутренних правовых границ и преследующего кибертеррористов независимо от их местонахождения. Теория R2P является адекватным основанием для введения универсальной юрисдикции в отношении кибертерроризма.

4.2. Решение: применимость концепции R2P для введения универсальной юрисдикции в отношении кибертерроризма

В правовой доктрине кибертерроризм рассматривается как международное зло (Margariti, 2017), поскольку его последствия для всеобщего мира и безопасности соответствуют таковым у ППЧ. Международное сообщество страдает от обоих видов преступлений (Margariti, 2017), однако кибернетическая составляющая отличает

кибертерроризм как современное зло (Perloff-Giles, 2018). Это эволюционировавшая разновидность преступлений против человечности, которая относится к категории «другие бесчеловечные деяния». Это очевидно, исходя из совпадения элементов кибертерроризма с контекстуальными элементами ППЧ, как показывает судебная практика⁶¹. Следовательно, универсальная юрисдикция необходима как глобальный механизм преследования и экстрадиции террористов. Однако противодействие применению универсальной юрисдикции⁶² требует наличия твердых оснований для ее применения. Такой опорой является теория R2P.

В представленном обзоре отмечается значимость теории R2P в международном праве. Данная концепция была разработана как инструмент защиты человечества. Основной целью R2P является защита человечества от злодеяний. Таким образом, ее применение для противостояния ППЧ доказывает ее значимость в международной доктрине и правовой практике. R2P, как считает Ройер, является гуманитарным инструментом предотвращения зла, поскольку оправдывает юридическое вмешательство для преследования виновных в ППЧ (Royer, 2021). При этом во главу угла ставится защита отдельных людей, а не сохранение суверенитета в Вестфальском понимании⁶³.

Ройер высоко оценивает гибкость механизма R2P, поскольку он позволяет достичь баланса с гуманитарными потребностями в предотвращении преступлений против человечности (Royer, 2021). Ученый переосмысливает R2P с позиции морали, поскольку это механизм противостояния злу (Royer, 2021). Как следствие, политическая воля не может противостоять нормам, которые на ней же и основаны. Напротив, концепция R2P объединяет политические интересы государств и мораль человечества в единый инструмент, направленный против злодеяний (Royer, 2021). Фактически это инструмент как политики, так и морали, который защищает людей от злодеяний (Royer, 2021). Такое переосмысление R2P доказывает правомерность использования норм международного права для пресечения ППЧ. Примечательно, что в своем видении R2P Ройер гармонично сочетает его с требованием государственного суверенитета, который в своей основе также является защитой от злодеяний, поскольку организует автономное управление внутренними делами государства. Следовательно, он борется с беспорядком внутри страны, которым могут воспользоваться злоумышленники для достижения своих целей (Royer, 2021). Таким образом, суверенитет отражает обязанность государства защищать граждан.

Как показывает практика МУС, коллективные обязательства государств побуждают их к принятию универсальных инструментов для искоренения ППЧ с целью обеспечения мира во всем мире⁶⁴. Природа универсальной юрисдикции не противоречит этой цели; преследование преступлений против человечности на международном уровне ограничивает их распространение и укрепляет правосудие. Поскольку концепция R2P допускает военное вмешательство для борьбы с ППЧ, она также оправдывает и судебное вмешательство, т. е. введение универсальной юрисдикции.

⁶¹ Prosecutor v Mucić et al, Trial judgment, 16 November 1998, IT-96-21-T, (Celebicić, Trial judgment), paras 521–522; Prosecutor v Karadžić, Trial judgment, 24 March 2016, IT-95-5/18-T, (Karadžić, Trial judgment), para 494; IT-97-25-T.

⁶² См. обсуждение в предыдущем разделе.

⁶³ Resolutions 1674 (2006), 63/308 (2009)⁶⁸ and 1894 (2009).

⁶⁴ Application of the Convention on the Prevention and Punishment of the Crime of Genocide (BiH v Serbia and Montenegro), 26 February 2007, ICJ Reports 2007 p. 43, para 166.

Поскольку, как показано в исследовании, кибертерроризм является преступлением против человечности, то концепция R2P должна оправдывать преследование кибертеррористов на международном уровне. Из этого следует, что суд или отдельный прокурор может преследовать кибертеррориста, находящегося на территории другой юрисдикции, если территориальная юрисдикция не проявляет к нему должного внимания. В этом случае, согласно объяснению Лауры Буренс (Burens, 2016), действует принцип горизонтальной взаимодополняемости. Концепция R2P оправдывает такое судебное вмешательство, поскольку международное сообщество обязано предотвращать ППЧ, как это установлено международным обычным правом. Судебное вмешательство для противодействия преступлениям против человечности лучше военного, поскольку оно повышает доверие к международному уголовному правосудию и устраняет угрозу человечеству со стороны кибертеррористов.

Заключение

Исследование посвящено изучению концепции R2P, анализу ее компонентов и комплексного представления о ней в международном праве. Данная концепция представляет собой превентивный инструмент для защиты человечества от злодеяний. О его значении можно судить по тому, что его применение было неоднократно санкционировано СБ ООН и международным сообществом для вмешательства в пресечение ППЧ. Это общий принцип международного права. Кроме того, юридический анализ доказывает гибкость механизма R2P, поскольку он применяется различным образом в каждом конкретном случае. Концепция R2P используется для обоснования военных операций и юридического вмешательства для преследования ППЧ. Изученные факты доказывают пригодность R2P для выполнения данной задачи.

Также в исследовании анализируется кибертерроризм. Это современная преступная деятельность, наносящая ущерб государствам. В доктрине он рассматривается как общий враг человечества, поскольку угрожает миру и безопасности во всем мире. Анализируя элементы этого явления, мы сопоставляем их с контекстуальными элементами ППЧ и делаем вывод об их конгруэнтности. Это означает, что кибертерроризм является преступлением против человечности согласно Римскому статуту. Категория «другие бесчеловечные деяния» распространяется и на кибертерроризм. Следовательно, международное сообщество должно принять меры по преследованию и наказанию кибертеррористов, чтобы устранить их безнаказанность.

Внешнее судебное вмешательство осуществляется в международном частном праве посредством универсальной юрисдикции. Она включает в себя использование национальных судебных инструментов в рамках других юрисдикций, поэтому сталкивается с рядом препятствий со стороны государств и даже региональных организаций. Эти препятствия сводят на нет международно-правовые усилия по пресечению кибертерроризма. Таким образом, необходимо найти адекватное юридическое обоснование универсальной юрисдикции, которое открыло бы международному сообществу путь к преследованию кибертеррористов.

Далее в работе представлен принцип R2P как необходимое обоснование универсальной юрисдикции в отношении кибертерроризма. Поскольку кибертерроризм представляет собой угрозу миру и безопасности во всем мире, международное сообщество должно принять меры по его искоренению с помощью механизмов универсальной юрисдикции. Такое вмешательство соответствует нормам международного права, так как обеспечивает защиту прав человека, что является его главной целью.

Наконец, представленное исследование устраняет разрыв между нормами международного публичного права и международного частного права, применяя теорию R2P из первого для обоснования универсальной юрисдикции из второго. Такое сочетание демонстрирует взаимодополняемость отраслей международного права, что служит глубокому пониманию международных киберпроблем.

Список литературы

- Adem, S. H. (2019). Palestine and the International Criminal Court. In Werle, G., & Vormbaum, M. (Eds.), *International Criminal Justice Series*, 21. T.M.C. Asser Press, The Hague. <https://doi.org/10.1007/978-94-6265-291-0>
- Albahar, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science and Engineering Ethics*, 25(4). <https://doi.org/10.1007/s11948-016-9864-0>
- Atadjanov, R. (2019). Humanness as a Protected Legal Interest of Crimes Against Humanity. Conceptual and Normative Aspect. In G. Werle, & M. Vormbaum (Eds.), *International Criminal Justice Series*, 22. T.M.C. Asser Press, The Hague. <https://doi.org/10.1007/978-94-6265-299-6>
- Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy*, 54, 138. <https://doi.org/10.1007/s12115-017-0114-0>
- Azubuibe, E. C. (2023). Principle of Responsibility to Protect: Implications for Sovereignty. In E. Duruigb, R. Chibueze, & S. G. Ogbodo (Eds.), *International Law and Development in the Global South* (pp. 55–77). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-13741-9_5
- Bellamy, A. (2018). Responsibility to Protect: Justice and Responsibility—Related but Not Synonymous. In J. Waterlow & J. Schuhmacher (Eds.), *War Crimes Trials and Investigations* (pp. 263–299). Cham, Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-64072-3_9
- Blešić, J. (2022). Aut Dedere Aut Judicare in International and Domestic Law. In *Protection of human rights and freedoms in light of international and national standards, Contemporary Problems of the Legal System of Serbia* (pp. 213–224). The Faculty of Law, University of Belgrade.
- Broeders, D., Cristiano, F., & Weggemans, D. (2021). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy, *Studies in Conflict and Terrorism*. <https://doi.org/10.1080/1057610x.2021.1928887>
- Burens, L. (2016). Universal Jurisdiction Meets Complementarity: An Approach towards a Desirable Future Codification of Horizontal Complementarity between the Member States of the International Criminal Court. *Criminal Law Forum*, 27(1), 75–97. <https://doi.org/10.1007/s10609-016-9272-9>
- Cantini, N., & Zavialov, D. (2018). Fixing Responsibility to Protect: Lessons from and Proposals for the Case of Libya. *Peace Human Rights Governance*, 2(1), 75. <https://doi.org/10.14658/pupj-phrg-2018-1-4>
- Correia, V. J. (2022). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom, *SN Computer Sciences*, 3, 84. <https://doi.org/10.1007/s42979-021-00962-5>
- Delerue, F., Desforges, A., & Géry, A. (2019, April 23). A Close Look at France's New Military Cyber Strategy. *War on the Rocks*. <https://clck.ru/36ktrj>
- Ercan, P. G. (2022). *The Responsibility to Protect Twenty Years On: Rhetoric and Implementation*. Palgrave Macmillan, Cham. <https://doi.org/10.1007/978-3-030-90731-0>
- Fehl, C. (2015). Probing the Responsibility to Protect's Civilian Dimension: What Can Non-Military Sanctions Achieve? In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 39–57). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1.
- Henschke, A. (2021). Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat. In A. Henschke, A. Reed, S. Robbins, & S. Miller (Eds.), *Counter-Terrorism, Ethics and Technology' Advanced Sciences and Technologies for Security Applications*. Springer. <https://clck.ru/36ktsa>
- Hobbs, H. (2017). Towards a Principled Justification for the Mixed Composition of Hybrid International Criminal Tribunals. *Leiden Journal of International Law*, 30(1), 177. <https://doi.org/10.1017/s092215651600056x>
- Holvoet, M., & Mema, M. (2015). The International Criminal Court and the Responsibility to Protect. In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 21–38). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1. https://doi.org/10.1057/9781137364401_3
- Kittichaisaree, K. (2017). Future Prospects of Public International Law of Cyberspace. In K. Kittichaisaree, *Public International Law of Cyberspace* (pp. 335–356). Springer. <https://clck.ru/36ktuq>

- MacNeil, G. (2021). Legality Matters: Crimes Against Humanity and the Problems and Promise of the Prohibition on Other Inhumane Acts. In G. W., & M. Vormbaum (Eds.), *International Criminal Justice Series*, 28. T.M.C. Asser Press, The Hague. <https://doi.org/10.1007/978-94-6265-443-3>
- Maguir, R. (2022). Prosecuting Crimes Against Humanity: Complementarity, Victims' Rights and Domestic Courts. *Criminal Law and Philosophy*, 17, 669–689. <https://doi.org/10.1007/s11572-022-09648-2>
- Margariti, S. (2017). Defining International Terrorism: Between State Sovereignty and Cosmopolitanism. In G. Werle, L. Fernandez, & M. Vormbaum (Eds.), *International Criminal Justice Series*, 15 (pp. 1–26). T.M.C. Asser Press, The Hague. ISBN 978-94-6265-204-0. <https://clck.ru/36ktwV>
- Mung'omba, I. (2022). Universal Jurisdiction as a Tool in Promoting Accountability for International Crimes in Africa: Exploring the Significance of Hissene Habre's Conviction. In E. C. Lubaale, & N. Dyani-Mhango (Eds.), *National Accountability for International Crimes in Africa* (pp. 91–114). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-88044-6_4
- Nyawo, J. (2023). The Scope and Application of Universal Jurisdiction: A Synopsis of African States' Positions and Proposals During Plenary Sessions in the Sixth Committee of the United Nations General Assembly. In T. B. K. Sendze, A. Adeboyejo, S. Ugwu, & H. Morrison (Eds.), *Contemporary International Criminal Law Issues. Contributions in Pursuit of Accountability for Africa and the World* (pp. 213–262). Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-555-3_7
- Park, T. J., & Switzer, M. (2020, May). R2P & Cyberspace: Sovereignty as a Responsibility. In *The 12th International Conference on Cyber Conflict*. Tallin, Estonia. <https://doi.org/10.23919/cycon49761.2020.9131729>
- Perloff-Giles, A. (2018). Transnational Cyber Offenses: Overcoming Jurisdictional Challenges. *Yale Journal of International Law*, 43(4), 191–227. <https://clck.ru/36ktyQ>
- Quigley, J. (2023). Prohibition of Palestine Arab Return to Israel as a Crime Against Humanity. *Criminal Law Forum*, 38. <https://doi.org/10.1007/s10609-022-09450-8>
- Royer, Ch. (2021). A Responsibility to Protect Humanity from Evil. In *Evil as a Crime Against Humanity. Ser. International Political Theory* (pp. 81–130). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-53817-0_3
- Schmitt, M. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139169288>
- Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2021). Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment, *British Journal of Political Science*. <https://doi.org/10.1017/s0007123420000812>
- Soler, Ch. (2019). *The Global Prosecution of Core Crimes under International Law*. T.M.C. Asser Press, The Hague. <https://doi.org/10.1007/978-94-6265-335-1>
- Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In K. Stoddart (Ed.), *Cyberwarfare: Threats to Critical Infrastructure* (pp. 351–399). Springer International Publishing. https://doi.org/10.1007/978-3-030-97299-8_6
- Tsilonis, V. (2019). *The Jurisdiction of the International Criminal Court*. Springer Nature Switzerland, Gewerbestrasse, Switzerland. <https://doi.org/10.1007/978-3-030-21526-2>
- Werle, G., & Jeßberger, F. (2014). *Principles of International Criminal Law* (4th ed.). Oxford University Press. ISBN 9780198826859. <https://goo.su/Xwzm>
- Wyatt, S. J. (2019). The Responsibility to Protect and Habermas: Theory of Constitutionalisation with a “Cosmopolitan Purpose”. In *The Responsibility to Protect and a Cosmopolitan Approach to Human Protection* (pp. 151–176). New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-00701-0_6

Сведения об авторе



Абделькарим Яссин Абдалла – судья, суд общей юрисдикции в Луксоре

Адрес: 82516, Египет, г. Сохаг, Мадинат Нассер, ул. Ахмим Сохаг, Нью Касалови Хотел

E-mail: yassinabdelkarim91@gmail.com

ORCID ID: <https://orcid.org/0000-0001-7388-1337>

Конфликт интересов

Автор сообщает 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: 10.77.51 / Отдельные виды преступлений

Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 23 июля 2023 г.

Дата одобрения после рецензирования – 25 октября 2023 г.

Дата принятия к опубликованию – 30 ноября 2023 г.

Дата онлайн-размещения – 15 декабря 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.43>

Employing the Responsibility to Protect (R2P) to Impose Universal Jurisdiction Regarding Cyber-Terrorism

Yassin Abdalla Abdelkarim

Luxor Elementary Court
Sohag, Egypt

Keywords

crimes against humanity,
cybersecurity,
cyberspace,
cyberterrorism,
digital technologies,
human rights,
international private law,
international public law,
jurisdiction,
law

Abstract

Objective: the development of wireless technologies and digital infrastructure has radically changed the human habitat, giving rise to a new type of space – a cyberspace. The uniqueness and peculiarities of this environment, including anonymity, boundlessness and problems related to the determination and establishment of jurisdiction, have become a breeding ground for the emergence of a new global threat – cyberterrorism. The latter is characterized by a high level of latency, low detection rate and incomparably greater danger than “real world” crimes. Countering new forms of crime has required the development of universal tools that overcome the limitations of traditional jurisdiction and allow states to prosecute terrorists in cyberspace. Identifying the relevant tools and identifying the political-legal obstacles to their implementation is the objective of this study.

Methods: to achieve the set goal the formal-legal method was used to analyze legal sources, including judicial practice, national legislation, and international acts. The doctrinal approach was also used, which allowed, on the basis of scientific works and theoretical constructions, explaining the complexity of the modern phenomena and predicting their future development. This said, the main focus is on criminals to prove their antagonism with humanity in accordance with theoretical views. Finally, the study analyzes the theories of universal and traditional jurisdiction and how they are applied to prosecute terrorists.

© Abdelkarim Y. A., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Results: the paper provides a critical analysis, reviewing and adapting the concept of jurisdiction as applied to a global, borderless and decentralized digital environment (cyberspace) and to the struggle against new forms of terrorism (cyberterrorism). Various jurisdictional models applicable in cyberspace are presented. The author bridges the gap between the main branches of law: international private law and public law by linking, in relation to cyberterrorism, the two theories: the “responsibility to protect” (R2P) theory and the application of universal jurisdiction. The trends of universal jurisdiction development are revealed.

Scientific novelty: the study develops the accumulated scientific knowledge while justifying the introduction of foreign jurisdiction in a state territory to prosecute cyberterrorists. It also establishes a link between the theory of universal jurisdiction in private international law and the “responsibility to protect” (R2P) theory in public international law, recognizing the latter as a relevant basis for the introduction of universal jurisdiction over cyberterrorism. Such traditional concepts as sovereignty and jurisdictional independence are reviewed. The gap related to the consideration of cyberterrorism as a crime against humanity in international law is bridged.

Practical significance: the implementation of the proposed conclusions will contribute to the strengthening of international prosecution of cyberterrorism and harmonize the international and national legal tools to struggle against this crime.

For citation

Abdelkarim, Y. A. (2023). Employing the Responsibility to Protect (R2P) to Impose Universal Jurisdiction Regarding Cyber-Terrorism. *Journal of Digital Technologies and Law*, 1(4), 994–1022. <https://doi.org/10.21202/jdtl.2023.43>

References

- Adem, S. H. (2019). Palestine and the International Criminal Court. In Werle, G., & Vormbaum, M. (Eds.), *International Criminal Justice Series*, 21. T.M.C. Asser Press, The Hague. <https://doi.org/10.1007/978-94-6265-291-0>
- Albahar, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science and Engineering Ethics*, 25(4). <https://doi.org/10.1007/s11948-016-9864-0>
- Atadjanov, R. (2019). Humanness as a Protected Legal Interest of Crimes Against Humanity. Conceptual and Normative Aspect. In G. Werle, & M. Vormbaum (Eds.), *International Criminal Justice Series*, 22. T.M.C. Asser Press, The Hague. <https://doi.org/10.1007/978-94-6265-299-6>
- Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy*, 54, 138. <https://doi.org/10.1007/s12115-017-0114-0>
- Azubuikwe, E. C. (2023). Principle of Responsibility to Protect: Implications for Sovereignty. In E. Duruigh, R. Chibueze, & S. G. Ogbodo (Eds.), *International Law and Development in the Global South* (pp. 55–77). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-13741-9_5
- Bellamy, A. (2018). Responsibility to Protect: Justice and Responsibility—Related but Not Synonymous. In J. Waterlow & J. Schuhmacher (Eds.), *War Crimes Trials and Investigations* (pp. 263–299). Cham, Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-64072-3_9

- Blešić, J. (2022). Aut Dedere Aut Judicare in International and Domestic Law. In *Protection of human rights and freedoms in light of international and national standards, Contemporary Problems of the Legal System of Serbia* (pp. 213–224). The Faculty of Law, University of Belgrade.
- Broeders, D., Cristiano, F., & Weggemans, D. (2021). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy, *Studies in Conflict and Terrorism*. <https://doi.org/10.1080/1057610x.2021.1928887>
- Burens, L. (2016). Universal Jurisdiction Meets Complementarity: An Approach towards a Desirable Future Codification of Horizontal Complementarity between the Member States of the International Criminal Court. *Criminal Law Forum*, 27(1), 75–97. <https://doi.org/10.1007/s10609-016-9272-9>
- Cantini, N., & Zavialov, D. (2018). Fixing Responsibility to Protect: Lessons from and Proposals for the Case of Libya. *Peace Human Rights Governance*, 2(1), 75. <https://doi.org/10.14658/pupj-phrg-2018-1-4>
- Correia, V. J. (2022). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom, *SN Computer Sciences*, 3, 84. <https://doi.org/10.1007/s42979-021-00962-5>
- Delerue, F., Desforges, A., & Géry, A. (2019, April 23). A Close Look at France's New Military Cyber Strategy. *War on the Rocks*. <https://clck.ru/36ktrj>
- Ercan, P. G. (2022). *The Responsibility to Protect Twenty Years On: Rhetoric and Implementation*. Palgrave Macmillan, Cham. <https://doi.org/10.1007/978-3-030-90731-0>
- Fehl, C. (2015). Probing the Responsibility to Protect's Civilian Dimension: What Can Non-Military Sanctions Achieve? In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 39–57). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1.
- Henschke, A. (2021). Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat. In A. Henschke, A. Reed, S. Robbins, & S. Miller (Eds.), *Counter-Terrorism, Ethics and Technology' Advanced Sciences and Technologies for Security Applications*. Springer. <https://clck.ru/36ktsa>
- Hobbs, H. (2017). Towards a Principled Justification for the Mixed Composition of Hybrid International Criminal Tribunals. *Leiden Journal of International Law*, 30(1), 177. <https://doi.org/10.1017/s092215651600056x>
- Holvoet, M., & Mema, M. (2015). The International Criminal Court and the Responsibility to Protect. In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 21–38). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1. https://doi.org/10.1057/9781137364401_3
- Kittichaisaree, K. (2017). Future Prospects of Public International Law of Cyberspace. In K. Kittichaisaree, *Public International Law of Cyberspace* (pp. 335–356). Springer. <https://clck.ru/36ktuq>
- MacNeil, G. (2021). Legality Matters: Crimes Against Humanity and the Problems and Promise of the Prohibition on Other Inhumane Acts. In G. W., & M. Vormbaum (Eds.), *International Criminal Justice Series*, 28. T.M.C. Asser Press, The Hague. <https://doi.org/10.1007/978-94-6265-443-3>
- Maguir, R. (2022). Prosecuting Crimes Against Humanity: Complementarity, Victims' Rights and Domestic Courts. *Criminal Law and Philosophy*, 17, 669–689. <https://doi.org/10.1007/s11572-022-09648-2>
- Margariti, S. (2017). Defining International Terrorism: Between State Sovereignty and Cosmopolitanism. In G. Werle, L. Fernandez, & M. Vormbaum (Eds.), *International Criminal Justice Series*, 15 (pp. 1–26). T.M.C. Asser Press, The Hague. ISBN 978-94-6265-204-0. <https://clck.ru/36ktwV>
- Mung'omba, I. (2022). Universal Jurisdiction as a Tool in Promoting Accountability for International Crimes in Africa: Exploring the Significance of Hissene Habre's Conviction. In E. C. Lubaale, & N. Dyani-Mhango (Eds.), *National Accountability for International Crimes in Africa* (pp. 91–114). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-88044-6_4
- Nyawo, J. (2023). The Scope and Application of Universal Jurisdiction: A Synopsis of African States' Positions and Proposals During Plenary Sessions in the Sixth Committee of the United Nations General Assembly. In T. B. K. Sendze, A. Adeboyejo, S. Ugwu, & H. Morrison (Eds.), *Contemporary International Criminal Law Issues. Contributions in Pursuit of Accountability for Africa and the World* (pp. 213–262). Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-555-3_7
- Park, T. J., & Switzer, M. (2020, May). R2P & Cyberspace: Sovereignty as a Responsibility. In *The 12th International Conference on Cyber Conflict*. Tallin, Estonia. <https://doi.org/10.23919/cycon49761.2020.9131729>
- Perloff-Giles, A. (2018). Transnational Cyber Offenses: Overcoming Jurisdictional Challenges. *Yale Journal of International Law*, 43(4), 191–227. <https://clck.ru/36ktyQ>
- Quigley, J. (2023). Prohibition of Palestine Arab Return to Israel as a Crime Against Humanity. *Criminal Law Forum*, 38. <https://doi.org/10.1007/s10609-022-09450-8>
- Royer, Ch. (2021). A Responsibility to Protect Humanity from Evil. In *Evil as a Crime Against Humanity. Ser. International Political Theory* (pp. 81–130). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-53817-0_3

- Schmitt, M. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139169288>
- Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2021). Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment, *British Journal of Political Science*. <https://doi.org/10.1017/s0007123420000812>
- Soler, Ch. (2019). *The Global Prosecution of Core Crimes under International Law*. T.M.C. Asser Press, The Hague. <https://doi.org/10.1007/978-94-6265-335-1>
- Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In K. Stoddart (Ed.), *Cyberwarfare: Threats to Critical Infrastructure* (pp. 351–399). Springer International Publishing. https://doi.org/10.1007/978-3-030-97299-8_6
- Tsilonis, V. (2019). *The Jurisdiction of the International Criminal Court*. Springer Nature Switzerland, Gewerbestrasse, Switzerland. <https://doi.org/10.1007/978-3-030-21526-2>
- Werle, G., & Jeßberger, F. (2014). *Principles of International Criminal Law* (4th ed.). Oxford University Press. ISBN 9780198826859. <https://goo.su/Xwzm>
- Wyatt, S. J. (2019). The Responsibility to Protect and Habermas: Theory of Constitutionalisation with a “Cosmopolitan Purpose”. In *The Responsibility to Protect and a Cosmopolitan Approach to Human Protection* (pp. 151–176). New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-00701-0_6

Author information



Yassin Abdalla Abdelkarim – Judge, Luxor Elementary Court

Address: New Casalovy Hotel Street, Akhmim Sohag Street, Madinat Nasser, 82516, Sohag, Egypt

E-mail: yassinabdelkarim91@gmail.com

ORCID ID: <https://orcid.org/0000-0001-7388-1337>

Conflicts of interest

The authors declare 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 – July 23, 2023

Date of approval – October 25, 2023

Date of acceptance – November 30, 2023

Date of online placement – December 15, 2023