Научная статья
УДК 34:004:341.4:004.8
EDN: https://elibrary.ru/nnftqi
DOI: https://doi.org/10.21202/jdtl.2024.46

Противодействие кибератакам: пробелы международного права и перспективы их преодоления

Мохаммад Минхазур Рахман ✉

Государственный университет Бангладеш, Дакка, Бангладеш

Тапос Кумар Дас

Джахангирнагарский университет, Дакка, Бангладеш
Городской университет Гонконга, Гонконг

Ключевые слова

кибератака,
киберпреступность,
международная конвенция,
международное право,
права человека,
право,
принцип должной осмотрительности,
принцип соразмерности,
принципы международного права,
цифровые технологии

Аннотация

Цель: категорирование кибератак в национальном и международном правопорядках и определение юридических мер противодействия им на международном уровне.

Методы: представлены доктринальным юридическим анализом, формально-юридическим, сравнительно-правовым методами, синтезом, индукцией, дедукцией, а также методикой правового прогнозирования и моделирования. Исследованию подверглись международно-правовые документы и акты национального законодательства, судебные прецеденты, доктринальные источники.

Результаты: в статье определены юридические последствия кибератак, выявлены трудности определения и привлечения лиц и организаций к ответственности за их совершение, обозначены национальные меры противодействия кибератакам на основе принципа пропорциональности, систематизированы международно-правовые основы реагирования на кибератаки. Основное внимание в работе уделено актуальным проблемам выявления и проверки кибероружия, установления международных стандартов его использования, разработки методов разоружения или ограничения наступательных кибервозможностей. Поставлен вопрос обеспечения гуманитарной деятельности, защиты важнейших объектов инфраструктуры, а также населения с помощью мер кибербезопасности в военное время. Проанализированы правовые основы и выявлены пробелы и иные дефекты действующего регулирования в осуществлении юрисдикции в таких областях кибердеятельности, как международные операции, локализация данных и экстерриториальное исполнение национального законодательства.

✉ Корреспондирующий автор

Разработаны и описаны параметры, в рамках которых государства вправе проводить упреждающие кибероперации для предотвращения или сдерживания кибератак (киберконтрмеры), основными из которых являются проявление должной осмотрительности, законность принятии решения о применении киберконтрмер, соразмерность защиты от последствий совершения противоправных действий.

Научная новизна: обусловлена представленными в статье прогрессивными решениями в области международно-правового регулирования принятия государствами киберконтрмер в ответ на киберпреступления, сформулированными с учетом влияния обозначенных мер противодействия на права и свободы человека и гражданина, в том числе такие как право на неприкосновенность частной жизни и свобода слова.

Практическая значимость: результаты проведенного исследования могут быть взяты за основу при разработке и совершенствовании международно-правовых инструментов в области борьбы с кибератаками и обеспечения кибербезопасности, а также могут послужить образцом для национального законодателя при проектировании правотворческих решений противодействия киберпреступлениям.

Для цитирования

Рахман, М. М., Дас, Т. К. (2024). Противодействие кибератакам: пробелы международного права и перспективы их преодоления. *Journal of Digital Technologies and Law*, *2*(4), 973–1002. https://doi.org/10.21202/jdtl.2024.46

Содержание

Введение

Участившиеся кибератаки представляют серьезную угрозу для безопасности государств в современном мире. Страны пытаются понять, как защитить себя от кибератак, а правовые последствия кибернападений и мер противодействия им стали важным объектом изучения. Данное исследование рассматривает многочисленные области международного права, относящиеся к правовым последствиям и проблемам, связанным с различными аспектами контрмер в кибервойне. Основным препятствием для решения указанных проблем является определение лиц или организаций, ответственных за кибератаки (Etzioni & Rice, 2015). Для разработки эффективных контрмер необходима корректная атрибуция кибератак. Однако последняя затруднена из-за природы Интернета, который позволяет сохранять анонимность и применять сложные тактики для сокрытия личности. В данном исследовании рассматриваются существующие правовые основы установления ответственности при атрибуции кибератак в контексте контрмер и предлагаются методы такого установления.

Еще одна важная тема, затронутая в данном исследовании, – соразмерность защиты от кибербоевых действий. Соблюдение соразмерности при оценке масштабов и серьезности контрмер становится еще более важным, когда страны отвечают на кибератаки. Учитывая асимметричный характер кибероперации и широкий сопутствующий ущерб, который они могут нанести, необходимо тщательно изучить правовые нормы для установления соразмерности мер противодействия (Roscini, 2014). Мы рассмотрим существующие правовые стандарты и концепции, а также их актуальность для киберконтрмер. Международное сотрудничество играет крайне важную роль перед лицом все более сложных и транснациональных киберугроз. В данном исследовании рассматриваются правовые структуры и процедуры, способствующие международному сотрудничеству в борьбе с кибератаками. Обмен информацией, координация действий и разработка эффективных мер по противодействию киберугрозам – все это требует сотрудничества между государствами.

В статье рассмотрены также преимущества и недостатки международного сотрудничества в области киберпротиводействия путем изучения существующих международных правовых инструментов и каналов сотрудничества. Хотя главными участниками кибервойн являются государства, растет значимость и других игроков – киберпреступников и организаций хактивистов [хактивист – хакер-активист – лицо, использующее компьютерные сети для распространения той или иной идеологии. – Прим. переводчика] (Buchan, 2012). Поэтому в данном исследовании оцениваются трудности привлечения негосударственных субъектов к ответственности за кибератаки и рассматриваются средства правовой защиты, доступные государствам для реагирования в рамках международного права. При проведении оборонительных или наступательных кибероперациий у государств возникают опасения по поводу возможного нарушения основных прав человека, таких как право на неприкосновенность частной жизни и свободу слова. Чтобы найти баланс между соображениями национальной безопасности и сохранением прав личности, необходимо изучить правовые основы и концепции на стыке регулирования прав человека и использования кибернетических контрмер. Кроме того, в работе анализируются параметры, в рамках которых государства могут законно проводить упреждающие кибероперации для предотвращения или сдерживания кибератак (Hollis & Finnemore, 2016).

В данном исследовании изучаются аспекты упреждающих киберконтрмер путем анализа существующих норм в области упреждающей обороны и их значимости для киберконтрмер. Рассмотрена необходимость должной осмотрительности как критерия подотчетности правительства в рамках киберпротиводействия, а также нормы и обязательства, налагаемые на государства при принятии решений о законности киберпротиводействия. Исследование проливает свет на потенциальные последствия и средства правовой защиты для правительств, участвующих в незаконной кибердеятельности. Мы также затронем такие аспекты, как трудности определения, проверки и регулирования кибероружия, стандарты использования кибероружия в контексте контрмер, а также правовые основы и перспективные процедуры разоружения или ограничения наступательных кибервозможностей (Liivoja & Väljataga, 2021). Кроме того, мы рассмотрим правовые основы, регулирующие разведывательные действия в киберпространстве, границы допустимого шпионажа, диапазон законных государственных интересов и их возможное влияние на международные отношения. Авторы утверждают, что такой подход способствует лучшему пониманию правовых последствий и трудностей сбора киберразведданных (Putman & Albright, 2018).

Кроме того, данное исследование показывает, как гарантии кибербезопасности могут помочь в обеспечении безопасности населения, жизненно важных объектов инфраструктуры и гуманитарной деятельности в военное время. Тем самым оно дает представление о возможных ролях и обязанностях государств и негосударственных субъектов в сохранении киберпространства во время войн путем изучения правовых требований государств и потенциальной взаимосвязи между кибербезопасностью и международным гуманитарным правом. Наконец, в работе рассматриваются трудности и юридические прецеденты, связанные с утверждением юрисдикции в отношении незаконных действий в киберпространстве. Рассматривая юрисдикционные проблемы, возникающие в результате трансграничных кибероперациий, локализации данных и экстерриториального применения национальных законов, это исследование, наконец, рассматривает возможности международного правового сотрудничества (Andrew & Bernard, 2021). Данное исследование направлено на дальнейшее создание правовых рамок и норм, регулирующих контрмеры в кибервойнах, путем изучения этих многочисленных и недостаточно изученных областей международного права, направленных на преодоление трудностей и неясностей, связанных с киберугрозами, и углубление знаний о правовых последствиях этого меняющегося ландшафта (Knowles & Thomas, 2016).

В работе рассмотрены три важных вопроса. Во-первых, исследуется вопрос законности и незаконности кибератак в соответствии с международным правом и международными договорами, а также сравниваются подходы различных юрисдикций и при различных условиях. Во-вторых, изучены существующие правовые рамки и методы, используемые государствами и международными организациями для реагирования на кибератаки и смягчения их последствий, а также определены и изучены потенциальные пределы кибернетического противодействия и стратегий самообороны с точки зрения международного права. В-третьих, учитывая динамичный характер глобальной цифровой экосистемы, в работе изучены пути более эффективного использования или изменения международного права и институтов для решения растущей проблемы кибератак.

Кроме того, в работе затронуты недостаточно исследованные вопросы, связанные с правовыми последствиями киберпротиводействия. Эти вопросы сложны и многомерны, что требует применения всеобъемлющих исследовательских методов. Для тщательного изучения темы в исследовании используются качественные исследовательские методологии и доктринальные подходы. Рассмотрены научные публикации, книги, юридические тексты, материалы прецедентного права и международные правовые документы (Wren & Wren, 1986). Эти источники дают представление о правовых основах, философии и аргументах в отношении различных контрмер в киберпространстве. Юридические последствия контрмер, трудности с установлением виновности и конкретные случаи кибератак будут рассмотрены с помощью тематических исследований. Мы покажем, как различные правовые системы и механизмы международного сотрудничества борются с кибератаками (Van Hoecke, 2011). Для определения актуальной ситуации и возможностей ее улучшения в работе проводится сопоставление ключевых международных договоров, соглашений и подходов к сотрудничеству, принятых на сегодняшний день. Чтобы прояснить правовые стандарты, нормы и принципы, регулирующие компоненты кибернетических контрмер, авторы изучают доктрину международно-правовых инструментов, таких как международные договоры, международное обычное право и соответствующие правовые принципы (Watkins & Burton, 2013).

Чтобы ответить на поставленные вопросы, также необходимы интерпретация и применение правовых норм и прецедентов. Исследование фокусируется на трудностях и юридических последствиях разработки мер реагирования на кибератаки. Основными ограничениями исследования выступает неполнота знаний и опыта авторов в этой постоянно развивающейся области (Tyler, 2017). Несмотря на это, можно ожидать, что работа значительно расширит знания о правовых последствиях и трудностях противодействия кибервойнам.

1. Проблемы, связанные с легальностью или нелегальностью кибератак

1.1. Проблема атрибуции кибератак

Поскольку кибератаки часто не оставляют после себя доказательств, установление виновности в таких преступлениях является сложной и долгосрочной операцией (Tsagourias & Farrell, 2020). Первым ее этапом будет определение источника кибератаки. По словам Michael Schmitt, установление виновности в кибератаках связано с трудностями. Ответственность за кибератаки не может определяться правовой системой. Однако существует множество правовых и инновационных подходов, помогающих в установлении виновности при кибератаках. Внедрение этих моделей и процедур позволит государствам более эффективно бороться с киберугрозами. По мнению Michael Schmitt, установить ответственность в случае кибератаки сложно из-за отсутствия единой правовой базы. Однако использование инновационных правовых подходов и методов повышает возможности стран по выявлению кибератак и разработке эффективных контрмер (Schmitt, 2013). Таким образом, в настоящее время существуют юридические инструменты, которые могут помочь в установлении виновности в случае чрезвычайных ситуаций в киберпространстве. James A. Lewis утверждает, что выявление лиц, совершивших

кибератаку, является важным первым шагом в реагировании на катастрофические события в киберпространстве. Если виновные не установлены, принятие надлежащих юридических, дипломатических или военных мер затруднительно. Анонимность Интернета и трудности с получением доказательств затрудняют установление тех, кто стоит за кибератаками. Тем не менее существует несколько вариантов решения проблемы идентификации. Это методы и ресурсы, с помощью которых государство может усилить свою защиту от киберугроз (Lewis, 2018). Это говорит о том, что, несмотря на трудности, существуют эффективные подходы к улучшению процессов атрибуции.

Аналогичным образом, в работе Gabriella Blum (Wittes & Blum, 2016) подчеркивается, что установление виновности в кибератаках является важным аспектом международного права. Сложно привлечь государство к ответственности за поведение в киберпространстве без установления виновности. Принципы ответственности государства, должной осмотрительности и соразмерности – это лишь некоторые из правовых рамок, которые используются для решения проблемы атрибуции атак через Интернет. Однако эти модели сложно применить на практике, так как для этого требуются более четкое формулирование и согласование правовых принципов определения виновных в кибератаках. Blum подчеркивает необходимость привлечения государств к ответственности за свои действия в киберпространстве и важность атрибуции с точки зрения международного права. Среди обсуждаемых ею правовых принципов, которые могут быть применены для установления виновности в кибератаках, – принципы ответственности государства, должной осмотрительности и пропорциональности (Wittes & Blum, 2016). Blum также признает сложность и реальные проблемы внедрения этих систем. Она подчеркивает важность более четкого определения и согласования правовых норм, регулирующих атрибуцию. Установление виновности имеет далеко идущие юридические последствия. Если одна страна докажет, что другая страна несет ответственность за кибератаку, то может подать на страну-нарушительницу в суд. Но государство не сможет предпринять юридические действия в случае кибератаки, если не определит, кто несет за нее ответственность (Ohlin et al., 2015).

Существуют и другие инновационные методы атрибуции кибератак в дополнение к существующим правовым рамкам. Киберкриминалистика занимается сбором и анализом цифровых доказательств, оставленных в результате кибератак. Эти данные могут быть использованы для установления лиц, совершивших кибероперации. Выявлению виновных в кибератаках способствует международное сотрудничество в области обмена информацией и ресурсами между государствами. В расследовании кибератак используется также сотрудничество государственного и частного секторов. Так, данные о кибератаках, полученные от частных лиц, могут быть переданы правительственным учреждениям и затем использованы для лучшего понимания и выявления киберугроз (Klimburg, 2018). Поскольку атрибуция кибератак является сложной и запутанной проблемой, нельзя полагаться на национальные правовые системы при установлении ответственности за них. Однако для установления виновности может быть использован ряд правовых рамок и нестандартных методов. Внедрение этих механизмов и методов позволит государствам эффективнее реагировать на киберугрозы.

1.2. Проблемы подотчетности негосударственных субъектов

Негосударственные организации, уклоняющиеся от ответственности за кибератаки, представляют значительные трудности для современного международного права. Юристы-международники отмечают трудности в судебном преследовании негосударственных субъектов за кибератаки. Однако в рамках международного права правительства располагают рядом юридических инструментов для реагирования на такие атаки. Среди жизнеспособных решений назовем подотчетность правительств, правовые контрмеры, целевые кибероперации и международное сотрудничество (Buchanan, 2017). Для выполнения своих международно-правовых обязательств государства должны тщательно продумывать законность и соразмерность своих действий.

Как отмечает Michael N. Schmitt (1999), кибероперации, осуществляемые негосударственными субъектами, подчиняются тем же традиционным нормам международного права, что и те, которые осуществляются государствами, а именно подотчетность государства и недопущение вмешательства. Schmitt подчеркивает, что обычные нормы международного права применимы и к негосударственным организациям, участвующим в кибератаках. Государство также может быть привлечено к ответственности за действия негосударственного субъекта, согласно принципу ответственности государства. Если негосударственные субъекты проводят кибероперации с территории одного государства против другого, также может применяться запрет на их участие. По мнению этого автора, одним из самых больших препятствий для привлечения негосударственных субъектов к ответственности за их действия является отсутствие четкой правовой базы, регулирующей атрибуцию кибератак негосударственным субъектам. Чтобы гарантировать законность и эффективность своих действий, государства должны сотрудничать в достижении общего понимания правовых стандартов, регулирующих кибероперации (Schmitt, 1999). Michael Schmitt обращает внимание на отсутствие четкой правовой базы и сложность установления причастности негосударственных субъектов к кибератакам. Термин «атрибуция» означает процедуру точного определения источника кибератаки. Трудно привлечь негосударственные структуры к ответственности за их поведение в отсутствие четко определенной правовой базы. Schmitt утверждает, что правительства должны сотрудничать в целях установления единых правовых норм в сфере кибердеятельности. Меры реагирования государств на киберугрозы могут быть успешными и законными, только если они основаны на общем понимании проблемы.

Таллиннское руководство 2.0 также предполагает, что законные меры, доступные государствам для борьбы с кибератаками, осуществляемыми негосударственными субъектами, включают дипломатические, экономические и юридические санкции. Согласно Таллиннскому руководству 2.0, правительства обладают широким спектром возможностей для реагирования на кибератаки со стороны негосударственных субъектов. Эти формы реагирования могут быть дипломатическими, экономическими или даже юридическими по своей природе, в зависимости от характера и обстоятельств правонарушения. Подобным же образом, как пишет Matthew C. Waxman, целенаправленные кибероперации применяются государствами против негосударственных субъектов, чтобы воспрепятствовать их деятельности, ослабить возможности и заставить их заплатить за свои атаки. По мнению этого автора, государства могут использовать целенаправленные кибероперации для пресечения операций и ресурсов негосударственных организаций, совершающих враждебные действия.

Также для предотвращения будущих кибератак на злоумышленников могут быть наложены штрафные санкции (Waxman, 2011). Однако для оценки законности и соразмерности таких мер следует руководствоваться нормами международного права.

1.3. Императив сотрудничества в отношении кибертерроризма

Согласно резолюции 71/256 Генеральной Ассамблеи ООН, государства должны работать сообща для обеспечения того, чтобы все усилия по предотвращению и ликвидации угрозы кибертерроризма были законными в соответствии со всеми применимыми международными договорами. В резолюции, принятой Генеральной Ассамблеей, также подчеркивается важность совместной работы правительств в борьбе с терроризмом, особенно кибертерроризмом, при соблюдении ими своих соответствующих обязательств по международному праву (Mačák, 2016). Поэтому, реагируя на кибератаки со стороны негосударственных субъектов, страны должны думать о международных правовых рамках. По словам Gabriella Blum, при любых попытках привлечь к ответственности негосударственные структуры отсутствие сотрудничества со стороны других стран является фундаментальной проблемой, которую необходимо решать. Эффективность мер реагирования государств зависит от их совместной работы по созданию механизмов сотрудничества. Gabriella Blum утверждает, что попыткам привлечь негосударственные структуры к ответственности за кибератаки препятствует отсутствие сотрудничества со стороны других стран. При борьбе с киберугрозами, исходящими от негосударственных субъектов, сотрудничество между правительствами имеет важное значение для сбора и совместного использования информации, обмена знаниями и координации операций. Blum утверждает, что для эффективного реагирования на киберугрозы странам необходимо создавать структуры для сотрудничества (Lewis et al., 2019). Примерами таких систем являются соглашения об обмене данными, проведении совместных исследований и координации ответных мер. Способность государств реагировать на негосударственные субъекты, участвующие в кибератаках, повышается за счет сотрудничества. Как обсуждалось выше, атрибуция кибератак негосударственным субъектам не регулируется какими-либо четкими международно-правовыми рамками. Эта двусмысленность усложняет задачу правительств по привлечению негосударственных субъектов к ответственности за их действия. Поскольку действия негосударственных субъектов сложно отследить и идентифицировать, принятие государствами мер против них затруднено, даже если негосударственные субъекты действительно причастны к нападению.

По ряду причин, включая политические соображения и опасения за последствия, страны не всегда сотрудничают с другими государствами в расследовании и наказании негосударственных субъектов. Невозможность совместной работы может затруднить привлечение негосударственных субъектов к ответственности. Несмотря на трудности, страны могут прибегать к правовым средствам при реагировании на кибератаки со стороны негосударственных субъектов. Проблема с негосударственным субъектом или государством, которое подозревается в укрывательстве негосударственного субъекта, может быть решена соответствующим государством с помощью дипломатических методов (Mazanec, 2015). Экономические санкции могут быть введены государствами как в отношении негосударственного субъекта, так и в отношении государства, которое предположительно предоставляет убежище

негосударственному субъекту. В ответ на кибератаки со стороны негосударственных субъектов государства могут прибегнуть к военным действиям. Однако этот выбор следует делать только тогда, когда все другие варианты будут исчерпаны, поскольку это может иметь серьезные последствия, включая эскалацию агрессии.

1.4. Проблемы прав человека при кибератаках

Кибератаки также могут негативно сказаться на правах человека, поскольку используются для самых разных целей, включая несанкционированный сбор данных, цензуру высказываний и сбои в работе систем. Последствия этого особенно существенны для таких категорий, как журналисты, активисты и представители маргинализированных сообществ. В контексте кибернетических мер противодействия существует ряд правовых механизмов, которые контролируют баланс между целями национальной безопасности и соблюдением прав человека (Kulesza & Balleste, 2015). Право на неприкосновенность частной жизни и возможность самовыражения – это лишь два из множества прав, гарантированных на международном уровне. Государства должны поддерживать эти свободы хотя бы в интересах национальной безопасности. Все вооруженные конфликты регулируются правом в области вооруженных конфликтов, также известным как международное гуманитарное право. Оно регулирует применение физических и виртуальных средств поражения. На национальном уровне может быть обеспечена более строгая защита прав человека; при определенных условиях предусмотрено ограничение применения контрмер в киберпространстве. Государства могут принимать различные меры, чтобы гарантировать соответствие своей деятельности в киберпространстве универсальным принципам прав человека. Право на неприкосновенность частной жизни и свободу слова – это два фундаментальных права, которые государства должны соблюдать при принятии контрмер в киберпространстве.

Принимаемые государствами кибернетические контрмеры должны соответствовать серьезности киберугрозы. Государства могут использовать любые кибернетические контрмеры, которые они считают подходящими для достижения этой цели (Watt, 2021). Применяя кибернетические контрмеры против любых государственных или негосударственных субъектов, государства должны принимать все возможные меры безопасности, чтобы гарантировать, что не пострадают гражданские лица или гражданское имущество. Любой ущерб, причиненный действиями государства в киберпространстве, должен быть компенсирован. В специальном докладе Совета ООН по правам человека по вопросу о поощрении и защите права на свободу мнений и их свободное выражение отмечалось, что права человека должны учитываться при разработке и внедрении политики и процедур кибербезопасности. В нем подчеркивалась необходимость соблюдения стандартов в области прав человека при осуществлении мер кибербезопасности и противодействия им. Меры должны быть законными, необходимыми, соразмерными и недискриминационными; они не должны выделять или дискриминировать каких-либо конкретных лиц или группы. Так, в деле Delfi AS v. Estonia ЕСПЧ неоднократно указывал, что право на свободное распространение и обсуждение любых идей, независимо от того, насколько они популярны или считаются неприемлемыми, является краеугольным камнем демократического общества. Это судебное дело показывает важность свободы слова в демократическом обществе (Wagner et al., 2019). В нем подчеркивается, что эта

свобода относится не только к общепринятой, но и потенциально спорной информации и мнениям. Поэтому, даже имея дело со спорными материалами, службы кибербезопасности должны обеспечить защиту этого права.

Кроме того, ст. 19 Международного пакта о гражданских и политических правах гласит, что каждый человек имеет право выражать свое мнение любым способом, который он считает нужным, будь то устно, письменно или печатно, средствами искусства или любыми другими средствами по своему выбору; это включает свободу искать, получать и распространять информацию и идеи любого характера, независимо от любых границ. Это положение закона подчеркивает широкий характер указанного права, включая в себя свободу доступа, потребления и распространения информации и идей любыми средствами массовой информации. Свобода выражения мнений и информации в цифровой сфере должна быть защищена от посягательств со стороны государств. Чтобы обеспечить проведение кибероперации в соответствии с международными нормами в области прав человека, требуется четкая и всеобъемлющая законодательная база (Mihr, 2017). Важное значение имеют такие аспекты этой системы, как подотчетность, мониторинг и судебный надзор. Прежде чем начинать какие-либо операции в киберпространстве, государства должны сначала провести всестороннюю оценку их воздействия на права человека. Они должны проанализировать, как ограничения повлияют на такие права, как неприкосновенность частной жизни и свобода слова, и убедиться, что эти ограничения не являются более жесткими, чем это абсолютно необходимо для достижения законных целей. Необходимо предусмотреть соблюдение надлежащих процессуальных норм, эффективные средства правовой защиты в случае предполагаемых нарушений, а также независимые и открытые методы надзора. Не ставя под угрозу законные интересы безопасности, государства должны информировать общественность о целях, масштабах и последствиях кибердеятельности, чтобы способствовать открытости и подотчетности. Им необходимо сотрудничать в глобальном масштабе для разработки руководящих принципов защиты прав человека в Интернете (Mihr, 2016). Созданию всеобъемлющих норм и предписаний способствует совместная работа с правительствами других стран, международными организациями и широкой общественностью. Государства могут найти баланс между правами человека и решением проблем национальной безопасности, обеспечив соответствие своей деятельности в киберпространстве международным нормам в области прав человека.

2. Масштабы и ограничения мер противодействия кибератакам

2.1. Установление пропорциональности при кибероперациях

Одним из краеугольных камней международного права является концепция пропорциональности, которая запрещает применение силы, несоразмерной серьезности угроз. К кибероперациям применяется то же правило, что и к любому другому виду военных действий. Соразмерность контрмеры должна оцениваться в свете специфики атаки, которую она призвана отразить. Ответная тактика, которая наносит больший ущерб, чем при первом нападении, скорее всего, будет считаться непропорциональной. Контрмера должна быть именно такой, какая необходима для предотвращения кибератаки. Непропорциональный ответ – это такой, который выходит за рамки того, что требуется для прекращения атаки. Контрмера не должна создавать больше проблем, чем решает. Если негативные последствия

контрмеры несоразмерны выгодам, то контрмера несправедлива. Применение идеи пропорциональности к кибероперациям может оказаться сложной задачей из-за уникального характера кибердеятельности (Dwan et al., 2022). Например, кибердеятельность может иметь непредвиденные последствия, и ее очень трудно отследить. Кибероперации создают уникальный набор проблем, когда речь заходит об определении соразмерности контрмер, что требует учета специфических особенностей кибератак и их последствий для концепции соразмерности. Актуальность современных принципов пропорциональности для киберопераций нашла отражение в трудах многих ученых в области международного права. Так, по словам Michael N. Schmitt, чтобы соответствовать стандарту пропорциональности, государства должны оценить потенциальный сопутствующий ущерб гражданским объектам и сопоставлять его с потенциальным военным преимуществом. Этот автор подчеркивает необходимость сопоставления военного преимущества, получаемого в результате кибероперaций, с прогнозируемым ущербом гражданским объектам. Кибератаки подпадают под эту концепцию пропорциональности, согласно которой правительства должны сопоставлять возможную военную выгоду с любым сопутствующим ущербом гражданской инфраструктуре, таким как критически важные системы или службы (Schmitt M., 2012).

Согласно Таллиннскому руководству 2.0 по международному праву в области кибероперaций, те кибероперации, которые наносят серьезный ущерб основной инфраструктуре или приводят к человеческим жертвам, могут рассматриваться как акт войны. Следовательно, при оценке потенциальных результатов таких кибероперaций необходимо использовать критерий пропорциональности. Ущерб критической инфраструктуре, гибель или ранения людей – все это признаки того, что кибероперация переросла в военный акт. Аналогичным образом, по словам Marco Roscini (2014), государство – участник конфликта не должно предпринимать кибератаку на гражданский объект, если прогнозируемый ущерб гражданскому населению или случайные повреждения будут несоразмерны ожидаемому военному преимуществу в соответствии с принципом пропорциональности. Этот автор подчеркивает важность ограничения последствий кибератак для невинных людей. При проведении кибероперации прогнозируемый ущерб гражданским объектам или лицам не должен превышать прогнозируемый военный выигрыш. Эта идея также актуальна в сфере кибервойн (Roscini, 2014). Также, по словам Christopher C. Joyner (2011), кибервойны должны регулироваться концепцией пропорциональности, которая гласит, что ответ участника боевых действий должен быть соизмерим с опасностью, исходящей от вооруженных сил противника. По словам этого автора, применение силы в кибервойне должно быть ограничено необходимостью и соизмеримо с опасностью, которую представляют военные возможности государства-мишени. Это означает, что кибероперации не должны наносить больше ущерба, чем это абсолютно необходимо для устранения текущей угрозы.

По мнению ученых (Frowe, 2022), пропорциональность в кибероперациях определяется путем оценки прогнозируемого военного преимущества по сравнению с ожидаемым ущербом гражданским объектам. Кибератаки отличаются от других видов атак и должны тщательно рассматриваться в контексте соразмерности из-за их потенциальной возможности нанести ущерб ключевой инфраструктуре или гражданскому населению. Уместность и законность кибероперaций в свете возможных последствий можно оценить, используя действующие правовые нормы и принципы,

относящиеся к категории соразмерности в вооруженных столкновениях. Кибератаки могут осуществляться государствами, располагающими гораздо меньшими ресурсами, чем у их целей. Возможности злоумышленника могут быть неизвестны или их трудно предсказать, что затрудняет определение того, являются ли контрмеры соразмерными или нет. Таким образом, две отличительные черты кибероперaций – сложность и непредсказуемость (Schmitt, 2011).

Из-за сложности прогнозирования всех возможных последствий может быть трудно определить, являются ли контрмеры соразмерными. Выявить источник кибератак также непросто, поскольку они могут быть предприняты откуда угодно. Это затрудняет определение цели для принятия контрмер. Кибератаки сложно оценить с точки зрения их масштаба и серьезности. Они могут нанести большой ущерб, но его степень трудно определить из-за их анонимности и сложности. Это затрудняет оценку адекватности ответных мер по отношению к серьезности атаки. Обоснование контрмер в киберпространстве является еще более сложной задачей. При большом количестве потенциальных способов реагирования на киберугрозы такое решение оказывается непростой задачей. Существует вероятность того, что при определенных обстоятельствах ответные действия окажутся чрезмерными. Прогнозирование потенциальных результатов контрмер в киберпространстве может быть затруднено.

2.2. Препятствия на пути глобального сотрудничества

Существует множество препятствий, которые мешают государствам совместно разрабатывать законные меры противодействия кибератакам. Деятельность в киберпространстве не регулируется каким-либо общепризнанным сводом законов. Эта неопределенность препятствует сотрудничеству государств в разработке эффективных мер противодействия. Атрибутировать кибератаку конкретному злоумышленнику часто бывает непросто. Поскольку страны не всегда уверены в том, на кого нацелена кибератака, это усложняет реагирование на такие удары (Friis & Ringsmose, 2016). Кибератаки могут иметь самые разнообразные преднамеренные и непредвиденные последствия. Однако сотрудничество государств для создания законной и эффективной киберзащиты имеет важное значение. Эксперты в области права указывают как на трудности, так и на возможные решения. Например, по словам Duncan Hollis (Hollis & Finnemore, 2016), взаимосвязь кибератак и уязвимостей требует международного сотрудничества для выработки решения, поскольку ни одно государство не может успешно справиться с этим в одиночку. Автор отмечает, что ни одно государство не может адекватно противостоять киберугрозам в одиночку, и указывает на взаимосвязанность, лежащую в основе киберпространства. Это подчеркивает необходимость совместной работы государств по обмену информацией, навыками и ресурсами для укрепления своей киберзащиты.

По мнению Christopher S. Yoo, затраты на сбор информации, координацию и обеспечение соблюдения норм могут быть снижены, а успешность мер кибербезопасности повышена за счет широкого распространения соответствующих данных от имени государств. Исследователь подчеркивает необходимость обмена информацией в области кибербезопасности между государствами. Это обеспечит кибербезопасность при одновременном сокращении расходов, связанных со сбором и координацией данных. Более эффективная защита от кибератак может быть достигнута за счет обмена информацией об угрозах, передовым опытом и

техническими навыками (Yoo & Blanchette, 2015). Международная стратегия США в отношении киберпространства предусматривает, что вместе с другими странами Соединенные Штаты будут укреплять киберстандарты, основанные на уважении прав человека, и стремиться снизить вероятность конфликтов, вызванных распространением и использованием информационно-коммуникационных технологий. Документ подчеркивает важность совместных усилий разных стран по распространению передовых практик в области кибербезопасности и поощрению ответственного поведения. Работая сообща, страны смогут создавать и внедрять стандарты и руководящие принципы для защиты прав человека, а также сделать Интернет более безопасным для всех.

Таллиннское руководство 2.0 предлагает такой же подход, отмечая, что соглашения о киберзащите между государствами могут содержать конкретные шаги по сотрудничеству, предпринимаемые для оказания помощи друг другу в случае кибератаки. Что касается кибернетических мер противодействия, то в Таллиннском руководстве 2.0 также рекомендуются двусторонние соглашения между странами. Такие соглашения служат основой для обмена информацией и ресурсами в случае кибернетического кризиса или кибератаки. Это укрепляет взаимное доверие и повышает эффективность реализации инициатив в области кибербезопасности (Tsagourias, 2012). Кроме того, согласно рекомендации Группы правительственных экспертов ООН (далее – ГПЭ ООН) по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности, для повышения способности всех стран предотвращать, расследовать, реагировать на инциденты, связанные с ИКТ, и восстанавливаться после них государства должны сотрудничать в разработке и осуществлении мер по наращиванию потенциала, включая взаимопомощь и сотрудничество. Сотрудничеству и координации между странами в значительной степени способствуют международные организации, такие как Организация Объединенных Наций (Henriksen, 2019).

Специалисты в области международного права отмечают преимущества и недостатки международного сотрудничества в разработке законных и эффективных средств защиты от киберугроз. Взаимосвязанность киберпространства требует от государств совместной работы, обмена данными и повышения их коллективной готовности. Многосторонние институты, такие как Организация Объединенных Наций, способствуют координации усилий и оказывают содействие в разработке стандартов и программ по наращиванию потенциала, тогда как двусторонние соглашения определяют конкретные шаги к сотрудничеству. Действуя совместно, государства укрепляют свои возможности в области кибербезопасности и могут реагировать на кибератаки, используя эти инструменты. Несмотря на имеющиеся сложности, существует ряд возможностей для международного сотрудничества в создании законных, но эффективных средств киберзащиты (Katagiri, 2021). Международные организации, такие как Организация Объединенных Наций, развивают сотрудничество между правительствами в целях разработки эффективных контрмер. Эти группы могут служить платформой для совместной разработки стратегий противодействия киберугрозам. Двусторонние соглашения между правительствами также помогают разработке эффективных мер противодействия. Эти соглашения служат основой для координации действий правительств в ответ на киберугрозы и обмена информацией о них.

Глобальный центр обмена информацией и анализа (Global Information Sharing and Analysis Centre, GISAC) – еще одна структура, которая способствует сотрудничеству между правительствами в целях выработки более эффективных ответных мер (Faga, 2017). Эти инструменты позволяют странам координировать свои действия в ответ на киберугрозы и обмениваться информацией о них. Существуют значительные препятствия для международного сотрудничества в разработке эффективных и правовых средств защиты от киберугроз. С другой стороны, существует также множество способов, позволяющих работать вместе для общего блага. Кибербезопасность – это общая ответственность, и сотрудничество между государствами должно приводить к принятию более эффективных мер защиты.

2.3. Правовые сложности в области упреждающей самозащиты

Превентивные кибероперации, проводимые странами для предотвращения или сдерживания возможных кибератак, являются предметом постоянных дискуссий, равно как и условия, при которых такие операции могут проводиться на законных основаниях. Существующие конвенции и правовые рамки, касающиеся упреждающей самообороны, не всегда применимы к кибератакам, и по этому вопросу нет достаточного согласия. Устав ООН, решение Международного суда по делу Никарагуа и обычное международное право являются наиболее важными нормами и правовыми рамками, относящимися к упреждающей самообороне (Dean, 2013). Применение силы против суверенитета или территориальной целостности государства прямо запрещено Уставом Организации Объединенных Наций. Напротив, ст. 51 Устава ООН разрешает государствам применять силу в целях самообороны. В деле Никарагуа международный суд постановил, что лицо имеет право применить силу в целях самообороны, даже если нападение еще не произошло. Тем не менее Международный суд подчеркнул, что риск нападения должен быть немедленным, всеобъемлющим и не оставляющим выбора средств и времени для обдумывания. Право на самооборону также признается международным обычным правом, которое содержит рекомендации в ситуациях самообороны, хотя их содержание не всегда очевидно. Некоторые юристы считают, что государства должны использовать все доступные дипломатические пути для урегулирования конфликта, прежде чем прибегать к силе. Однако другие утверждают, что правительства имеют право применять силу в целях самообороны перед лицом нападения, даже если дипломатические решения конфликта все еще возможны.

Продолжается дискуссия о том, применимы ли действующие нормы и правовые рамки, касающиеся упреждающей самообороны, при кибератаках (Lucas, 2016). Мнения экспертов о том, можно ли применять концепции самообороны в киберпространстве, разделились из-за особого характера кибератак. Сложность определения причин атак является основным препятствием для разработки стратегий самообороны в киберпространстве. В реальном мире установить личность преступника, совершившего нападение, обычно не составляет особого труда, однако отследить источник нападения в киберпространстве может быть непросто. Это снижает способность государств оценивать угрозы и осуществлять право на самооборону. Еще одна проблема, связанная с переносом традиционных концепций самообороны в киберпространство, заключается в определении того, насколько близка угроза нападения. В реальном мире обычно легко определить, произойдет ли нападение в ближайшее время. Однако оценить непосредственную угрозу нападения в киберпространстве

может быть непросто. Это усложняет для правительств вопрос о том, имеют ли они право осуществлять самооборону перед лицом неминуемой угрозы (Levite & Perkovich, 2017).

Превентивные кибероперации, при которых государство активно предпринимает действия, чтобы остановить или пресечь атаку, являются спорной темой для обсуждения среди экспертов. Существующие нормы и правовые рамки, касающиеся упреждающей самообороны, не всегда очевидны или уместны в киберпространстве, и по этому вопросу нет четкого консенсуса. Согласно решению по делу Nicaragua v. United States of America (1986), принятому Международным судом, в случае вторжения или другого вооруженного нападения каждое суверенное государство имеет право применить военные действия для защиты своей территории. Это подтверждает неотъемлемое право на самооборону. Международный суд постановил, что право на самооборону включает в себя способность принимать меры перед лицом непосредственной угрозы насилия (Travis, 2016), а также что действия по самообороне, включая применение силы, должны быть обоснованы.

По словам Michael Schmitt, чтобы применение силы в целях упреждающей самообороны было оправданным, оно должно быть необходимым, соразмерным и применяться в ответ на неминуемое незаконное вооруженное нападение. Ученый предполагает, что упреждающая самооборона оправдана только в тех случаях, когда применение силы необходимо и уместно, угроза вооруженного нападения неизбежна и законных альтернатив применению силы нет[1]. Аналогичным образом, Bruce Schneier утверждает, что государства должны избегать участия в упреждающих кибероперациях, поскольку они потенциально разрушительны и непредсказуемы. Странам будет сложнее работать сообща над решением проблем кибербезопасности, если эта напряженность усилится. Ученый считает, что превентивные кибероперации приведут к обострению споров и затруднят совместную работу стран по устранению угроз кибербезопасности (Schneier, 2013). В целом эти мнения юристов-международников подчеркивают, что ситуация с превентивными кибероперациями неоднозначна и законодательство в этой области все еще находится в стадии разработки. Единодушного мнения по этому вопросу нет. Однако ученые-юристы считают, что важнейшими критериями легитимности превентивных кибероперациий являются следующие: неизбежность угрозы, необходимость применения силы, пропорциональность применения силы и различие между комбатантами и гражданскими лицами.

Опасности и выгоды от проведения превентивных кибероперациий должны сопоставляться с этими правовыми ограничениями. Превентивные кибератаки чреваты разжиганием более масштабной войны (Ossoff, 2021). Они могут иметь тяжелые последствия, если нанесут ущерб международным связям и затруднят совместную работу правительств в области кибербезопасности. Ситуация с превентивными кибероперациями сложна, и выбор в пользу их применения должен приниматься в каждом конкретном случае. Правовые, стратегические и политические последствия таких операций должны тщательно рассматриваться государствами до их проведения.

---

[1] Schmitt, M. (2022, 24 May). The United Kingdom on International Law in Cyberspace. EJIL: Talk! https://clck.ru/3F3MMo

3. Инструментализация международного права и институтов для борьбы с кибератаками

3.1. Преодоление лакун в международных нормах кибербезопасности

Существующие международные организации пока не в состоянии справиться со сложностью и динамичностью киберугроз. Примером является ситуация с ГПЭ ООН. Усилиям ГПЭ по созданию добровольных нормативных рамок препятствует тот факт, что они основаны на консенсусе. Это замедляет их разработку и иногда приводит к тупиковым ситуациям в результате конкурирующих национальных интересов и геополитических конфликтов. Еще одной серьезной проблемой является неспособность существующего международного права выносить решения и применять санкции в отношении правительств, которые совершают кибератаки или содействуют им. Поскольку существующие процедуры обеспечения соблюдения основаны преимущественно на традиционных представлениях о военных действиях, имеются лакуны в институциональной защите государств, которые проводят враждебные кибероперации. Это подчеркивает необходимость в новой международной конвенции, которая более точно определяла бы незаконные действия в киберпространстве и обеспечивала эффективные механизмы судебного разбирательства и правоприменения. В связи с постоянно развивающимся характером технологий также требуется разработать новую международную конвенцию.

Современные технологические достижения опережают возможности существующего международного права и институтов по эффективному реагированию. Например, появление квантовых вычислений и кибератак, управляемых искусственным интеллектом, порождает новые проблемы, которые еще не учтены существующими системами. Конвенция, ориентированная на будущее, может принести пользу, если будет изначально разработана с учетом возможностей адаптации и гибкости, роста и развития параллельно с развитием технологий. Более того, идея глобального сотрудничества подчеркивает важность разработки новой международной конвенции (Gow et al., 2019). Кибербезопасность – это международная проблема, требующая согласованных усилий. Различные национальные интересы и отсутствие доверия между странами мешают существующим международным организациям наладить активное глобальное сотрудничество. Развитию сотрудничества, укреплению доверия и обеспечению коллективной кибербезопасности могут способствовать согласованные на глобальном уровне рамки, предусмотренные международной конвенцией. Отрадно, что существующие международные организации пытаются решить проблему кибератак. Однако из-за постоянно меняющегося характера киберугроз и ограничений существующих международных правовых и институциональных рамок реакция на эти риски до сих пор не была адекватной. Новая международная конвенция, направленная на противодействие киберугрозам, имеет большие перспективы. Эта система может стать прозрачной, всеобъемлющей и гибкой, чтобы способствовать международному сотрудничеству, определять преступные деяния и устанавливать процедуры правоприменения.

Принятие такой конвенции стало бы важным шагом на пути к более надежному и безопасному Интернету. Что касается урегулирования споров и толкования международного права, Международный суд ООН и другие международные судебные органы находятся в авангарде (Harrison Dinniss, 2012). Однако существует ряд

проблем, снижающих их эффективность и применимость в борьбе с кибератаками. Международный суд должен обладать юрисдикцией в отношении того или иного вопроса, чтобы выносить по нему решение, и это обычно достигается при сотрудничестве правительств участвующих стран. Однако установить причастных к кибератакам людей и заручиться согласием соответствующих государств довольно сложно, поскольку происхождение этих лиц часто неизвестно и они могут действовать из разных юрисдикций. При вынесении своих решений Международный суд и другие аналогичные суды часто ссылаются на прецеденты и устоявшиеся принципы международного права. Поскольку военные действия в киберпространстве еще находятся в зачаточном состоянии, ориентирами могут служить лишь несколько примеров. Учитывая сложность и новизну этой ситуации, суд может испытывать сложности с применением существующих правовых норм (Bucci, 2018).

Рассмотрение дел в международных судах может занимать годы из-за сложности соответствующего законодательства. Однако кибератаки происходят с головокружительной скоростью и требуют быстрого реагирования. Судебной системе трудно адекватно разрешать киберконфликты из-за несоответствия между темпами судебных разбирательств и быстро развивающимся киберпространством. Нет единого мнения о том, как следует толковать суверенитет, невмешательство и применение силы в соответствии с традиционным международным правом в контексте кибероперациий. В 2018 г. генеральный прокурор Великобритании Джереми Райт выступил с лекцией, в которой утверждал, что киберинфраструктура страны должна рассматриваться как часть ее суверенной территории[2]. Из-за этих несоответствий международные суды иногда выносят решения, противоречащие друг другу. Устав Организации Объединенных Наций, Женевские конвенции и некоторые другие нормативные документы, не имеющие обязательной силы, составляют в международном праве основу для определения допустимости действий. Проблемы атрибуции, причинения нефизического вреда и подотчетности правительства в киберпространстве нелегко решить с помощью этих законов, поскольку они были написаны задолго до появления Интернета. Например, легкость совершения кибератак затрудняет их отслеживание до государственного субъекта в случае их осуществления. Юридическая оценка таких операций еще более осложняется отсутствием ясности в отношении того, что представляет собой «вооруженное нападение» в киберпространстве.

Принятие новой Международной конвенции позволит ввести четкие определения, стандарты и нормы, адаптированные к цифровой среде (Nissenbaum, 2015). Существующие правовые рамки представляют собой серьезные препятствия для принятия мер противодействия кибератакам. Остается спорным вопрос о том, имеют ли правительства право на самооборону от кибератак в соответствии со ст. 51 Устава Организации Объединенных Наций. В отличие от традиционных боевых действий, нет единого мнения о том, являются ли такие действия в киберпространстве необходимыми или соразмерными (Cornish, 2021). Новая международная конвенция сделает возможным установление более четких стандартов для принятия контрмер, включая характерные для киберпространства концепции пропорциональности, необходимости и дифференциации. Организация Объединенных Наций

[2] Schmitt, M. (2022, 24 May). The United Kingdom on International Law in Cyberspace. EJIL: Talk! https://clck.ru/3F3MMo

и другие международные организации предприняли ряд важных шагов в борьбе с киберпреступностью. Однако они не всегда успешны из-за таких факторов, как противоречащие друг другу законы и вопросы юрисдикции. Чтобы должным образом противостоять кибератакам, необходимо использовать международное право и институты. Однако для этого потребуются масштабные изменения, чтобы адаптироваться к постоянно меняющемуся характеру киберугроз и справиться с вызовами, возникающими в цифровой сфере. Частоту и серьезность кибератак можно снизить путем принятия новых международных конвенций, которые бы определяли, стандартизировали и обеспечивали применение контрмер.

3.2. Необходимость перевода правовых стандартов в киберпространство

Из-за нетрадиционного характера кибероперациий к кибератакам и кибернетическим контрмерам может быть сложно применить традиционные правовые стандарты, такие как различение, соразмерность и военная необходимость. Например, к комбатантам и гражданским лицам следует относиться по-разному, и в соответствии с концепцией различения следует атаковать только военные объекты. Из-за анонимности и идентификации, присущих киберпространству, определение источника и типа атаки является основной проблемой в кибервойнах. Проведение различий в киберпространстве сопряжено с серьезными трудностями из-за дублирования военных и гражданских компьютерных систем, сетей и инфраструктуры. Также, согласно концепции пропорциональности, атака может быть предпринята только в том случае, если ожидаемое военное преимущество оправдывает риск для населения и гражданской инфраструктуры. В условиях кибервойны сложно точно оценить возможные последствия атаки и сопутствующий ущерб, который она может нанести. Непредвиденные вторичные последствия кибероперации и каскадные воздействия бывает трудно предвидеть из-за взаимосвязанной структуры компьютерных систем и сетей. Более того, для достижения законных военных целей может быть использована сила, однако чрезмерное применение силы запрещено в соответствии с концепцией военной необходимости (Singer & Friedman, 2014). Определение законной военной цели в кибервойне является проблематичным и сложным. Помимо обычных военных целей, целями кибероперациий являются ключевые объекты инфраструктуры, экономические системы и информационные сети. Поскольку последствия кибероперациий могут выходить далеко за рамки традиционных военных целей, определение того, когда в них отпадает необходимость, представляет собой значительную трудность.

По словам Michael Schmitt (2013), те же правила различения, соразмерности и военной необходимости, которые применяются в обычных конфликтах, применимы и к кибервойнам. Он утверждает, что стороны в боевых действиях должны видеть разницу между гражданскими лицами и комбатантами и наносить удары исключительно по первым. Стороны конфликта обязаны в соответствии с концепцией пропорциональности применять только тот уровень силы, который является необходимым и пропорциональным их ожидаемому военному преимуществу. Участвующие стороны обязаны в соответствии с концепцией военной необходимости применять силу не более, чем это требуется для достижения цели, которая может быть оправдана применением силы. По мнению указанного ученого, кибервойну можно рассматривать через ту же призму, что и обычную войну, то есть необходимо

руководствоваться концепциями различения, пропорциональности и военной необходимости. Он утверждает, что в случае кибератаки вовлеченные стороны также должны отличать военных от гражданских лиц и сосредоточить свои атаки на первых. Принцип пропорциональности диктует, что для достижения конкретной военной цели следует применять силу только в разумных масштабах. Согласно принципу военной необходимости, сила должна применяться только в случае абсолютной необходимости для достижения законной военной цели. Schmitt отмечает, что эти руководящие принципы позволят странам участвовать в кибероперациях, не нарушая международных норм (Schmitt, 2013).

Однако, по мнению профессора Cordula Droege (2012), особенности кибероперациий не позволяют применять традиционные критерии различения, пропорциональности и военной необходимости к киберконфликту. По его словам, кибератаки могут иметь непредвиденные последствия, и иногда их трудно идентифицировать. Ученый считает, что страны должны найти новые подходы к применению критериев различения, пропорциональности и военной необходимости к кибервойнам. Он утверждает, что эти критерии трудно применимы к кибероперациям из-за их специфического характера. Droege согласен с тем, что определение ответственности за последствия кибероперациий может быть сложной задачей. Поэтому, по его мнению, странам необходимо внедрять инновации, чтобы адаптировать эти идеи к кибервойнам (Droege, 2012). Сложность кибероперациий требует новых подходов и концепций. Более того, по словам Russel Buchan (Buchan, 2012), они должны интерпретироваться таким образом, чтобы учитывать особый характер кибероперациий. Последствия кибероперациий могут быть как физическими, так и нефизическими, объясняет ученый. По его словам, правительства должны проявлять осторожность при проведении кибероперациий. Buchan предлагает учитывать указанные критерии в качестве средства достижения справедливого баланса в киберконфликтах. Однако он отмечает, что эти понятия необходимо интерпретировать с учетом специфики кибероперациий. Как признает ученый, кибероперации могут иметь ряд конкретных и нематериальных последствий. Поэтому он предостерегает от нарушения норм осторожности и ответственности при проведении кибероперациий (Buchan, 2012).

3.3. Неадекватность традиционных принципов ведения войны в киберпространстве

Одной из самых больших проблем, связанных с созданием принципов ведения кибервойн, которые соответствовали бы традиционным боевым действиям, является атрибуция. Отследить источник или начало кибератаки не всегда возможно (Denardis, 2020). Это затрудняет привлечение государств к ответственности за эти действия и предотвращение атак до их начала. При адаптации традиционных методов разрешения конфликтов к цифровой среде сложно исключить непредвиденные последствия. Кибератаки могут иметь самые разнообразные физические и нефизические последствия. Например, атака на правительственную компьютерную сеть может привести к непреднамеренному отключению основных служб, таких как электросети или водоснабжение. Это усложняет задачу обеспечения разумности и уместности действий в киберпространстве. Операции в киберпространстве сложны, и их не всегда легко понять (Winterfeld & Andress, 2013). Из-за этого трудно применять концепции пропорциональности, дифференциации и военной необходимости. Иногда

бывает невозможно определить, направлена ли кибероперация против военного объекта или гражданского населения. Оценка возможных физических и нефизических последствий кибератак также может быть сложной задачей.

Существует ряд проблем, которые необходимо решить, прежде чем адаптировать традиционные принципы ведения вооруженных конфликтов к кибервойнам. Именно по этой причине кибервойне трудно дать точное определение, а также установить общепринятые принципы их ведения в глобальном масштабе. В сфере кибербезопасности отсутствует всемирная нормативно-правовая база, что препятствует совместной работе государств по борьбе с киберугрозами (Whyte & Mazanec, 2018). Темпы технического развития в киберпространстве очень высоки. Это затрудняет принятие новых законов и норм для своевременного устранения возникающих киберугроз. Несмотря на препятствия, необходимо приложить усилия для изменения норм ведения обычных боевых действий, чтобы они могли применяться к кибервойнам. Необходимы правила и конвенции по контролю за кибервойнами в связи с возрастающей опасностью, которую они представляют.

3.4. Сложности работы вне суверенных границ

По мнению Michael Schmitt (2012), правовые основы, определяющие юрисдикцию в отношении кибератак, сложны и находятся в процессе развития. Государства имеют значительную свободу действий в выборе того, как они будут осуществлять юрисдикцию в отношении кибероперации, и, как отмечает ученый, нет ни одной международной конвенции, которая бы напрямую решала этот вопрос. Schmitt утверждает, что нации могут руководствоваться различными всеобъемлющими принципами, такими как концепции территориальности, гражданства и универсальности (Schmitt M. N., 2012). Способность национального государства регулировать поведение в Интернете внутри своих границ основана на идее территориальности. Это означает, что, даже если жертвы киберпреступления находятся в другой стране, виновные могут быть привлечены к ответственности государством, в котором было совершено преступление (Schmitt, 2014). Принцип гражданства гласит, что страна несет ответственность за преступные деяния своих граждан в любой точке мира, в том числе когда они совершаются через Интернет. Таким образом, независимо от местонахождения жертв, государство может выдвигать обвинения против своих граждан, совершающих киберпреступления. Согласно принципу универсальности, любое киберпреступление, которое соответствует определению преступления по международному праву, может преследоваться в судебном порядке любым государством, независимо от того, где и кем было совершено преступление. Киберпреступников можно преследовать в судебном порядке в государстве, даже если они не являются резидентами этого государства, если их действия квалифицируются как преступления по международному праву, а их жертвы находятся в другой стране (Shackelford, 2014).

Однако Thomas J. Holt и соавторы (Holt et al., 2015) утверждают, что установление юрисдикции в отношении действий, совершаемых в киберпространстве, сопряжено с серьезными трудностями. Он указывает на трудности, связанные с отслеживанием происхождения кибератак и их возможного воздействия на глобальном уровне. Исследователь подчеркивает, что для того, чтобы государства могли осуществлять контроль за кибератаками, им необходимо внедрять новые формы сотрудничества. Это связано с тем, что иногда бывает трудно определить источник кибератаки, когда она только начинается. В результате становится все

сложнее привлекать государства к ответственности и предотвращать возможные нападения. Возможность непредвиденных последствий является еще одной трудностью при установлении юрисдикции в отношении кибератак. Последствия кибератак, как физические, так и иные, могут быть весьма разнообразными. Например, атака на правительственную компьютерную сеть может привести к непреднамеренному отключению основных служб, таких как электросети или водоснабжение (Shackelford, 2012). Это усложняет задачу обеспечения разумности и уместности действий в киберпространстве. По словам Peter M. Shane (Shane & Hunker, 2013), по мере роста масштабов кибератак трудности в установлении и применении юрисдикции в отношении них будут только возрастать. По его мнению, государствам необходимо прибегнуть к нестандартным подходам, чтобы справиться с трудностями, связанными с осуществлением их полномочий в отношении онлайн-активности. Ожидается, что трудности, связанные с осуществлением юрисдикции в отношении кибероперaций, будут возрастать по мере дальнейшего развития кибертехнологий. Для преодоления этих трудностей государствам потребуется внедрять новые формы сотрудничества и координации (Shane & Hunker, 2013). Им также придется разработать ряд совершенно новых норм для контроля поведения в Интернете.

Отличаются сложностью и постоянно развиваются также проблемы юрисдикции, связанные с кибероперациями. Поскольку деятельность в киберпространстве не регулируется единой международной конвенцией, правительства отдельных стран имеют значительную свободу действий в определении сферы своей юрисдикции. Однако существует ряд общих принципов, которые могут использоваться для регулирования поведения государств. Эти понятия включают территориальность, национальную принадлежность и универсальность. Существуют значительные трудности в обеспечении соблюдения юрисдикции в отношении киберактивности (Roscini, 2010). Лица, стоящие за кибератаками, не всегда очевидны, а последствия их действий могут ощущаться по всему миру. Успешное определение юрисдикции в отношении кибератак требует новых форм сотрудничества между государствами. По мере расширения масштабов кибератак трудности с определением юрисдикции в отношении них, вероятно, сохранятся. Проблемы, связанные с установлением государственной власти над онлайн-активностью, требуют от правительств принятия упреждающих мер. В сфере кибербезопасности отсутствует всемирная нормативно-правовая база. Это препятствует совместной работе государств по борьбе с киберугрозами. Темпы технического развития в киберпространстве очень высоки (Gheciu & Wohlforth, 2018). Это затрудняет принятие новых законов и норм для своевременного устранения возникающих киберугроз. В рамках международного сотрудничества проблемы кибербезопасности решаются недостаточно активно. Необходимы совместные усилия по созданию и внедрению глобальных стандартов поведения в киберпространстве.

Заключение

В данном исследовании рассмотрены правовые последствия и трудности, связанные с кибератаками и мерами противодействия этим атакам в киберпространстве. Авторы подчеркивают, насколько сложно точно определить источник кибератак и насколько важно учитывать соразмерность при разработке контрмер в киберпространстве. В исследовании также обсуждается влияние кибернетических контрмер на права человека, правовые последствия контрмер против негосударственных

субъектов и правовые основы международного сотрудничества. Кроме того, рассмотрены правовые параметры превентивных кибероперациий, уровень подотчетности государства, трудности определения и проверки кибероружия, регулирующие структуры для разведывательных операций, роль мер кибербезопасности в защите гражданского населения и критически важной инфраструктуры, трудности установления юрисдикции в отношении кибердеятельности, а также взаимосвязь между кибербезопасностью и правом на развитие. Считая эти вопросы недостаточно изученными в рамках международного права, исследователи надеются внести свой вклад в формирование правовых систем и норм, регулирующих контрмеры в кибервойнах, способствуя тем самым инклюзивному и устойчивому росту при сохранении прав личности и международной кибербезопасности. По мере того как мир становится все более взаимосвязанным, риски, связанные с киберпространством, остаются насущной проблемой. Национальные границы становятся неэффективными, а существующие международные правовые системы сталкиваются с различными вызовами. Цифровая сфера является «серой зоной» с неопределенными правовыми принципами, что осложняет вопрос о том, являются ли кибератаки на самом деле преступными или нет. Отсутствие консенсуса в отношении определения кибератак и того, как общепринятые принципы международного права должны применяться к этим проблемам современности, является существенным пробелом в правовой системе. Для решения сложных проблем киберпространства требуется отдельная международная конвенция. Существующие рамки имеют свои ограничения и юрисдикционные проблемы, которые должна прояснить подобная конвенция. Это сложная задача, но ее необходимо решить для поддержания глобальной стабильности в эпоху, когда войны с такой же вероятностью будут вестись в Интернете, как и на земле. Международные организации пытались решить проблему кибератак, однако надлежащего ответа пока не удается добиться из-за постоянно меняющегося характера киберугроз и ограничений, налагаемых существующим международным правом и институциональными рамками. Новая международная конвенция, направленная на борьбу с киберугрозами, вселяет надежду на решение этого вопроса. Эта конвенция должна быть прозрачной, всеобъемлющей и гибкой, чтобы способствовать международному сотрудничеству, дать четкие определение уголовным деяниям и установить процедуры обеспечения их соблюдения. Такая конвенция стала бы огромным шагом вперед в деле повышения защищенности и безопасности Интернета. Поэтому важно пересмотреть и адаптировать существующую правовую инфраструктуру или изучить возможность создания специального международного органа, который мог бы эффективно реагировать на особенности военных действий в киберпространстве.

Список литературы

Andrew, J., & Bernard, F. (Eds.) (2021). *Human Rights Responsibilities in the Digital Age: States, Companies, and Individuals*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509938865

Bucci, S. (2018). Strategic Cyber Deterrence: The Active Cyber Defense Option by Scott Jasper. Rowman & Littlefield, 2017, 255 pp. *Strategic Studies Quarterly*, *12*(2), 134–135.

Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law*, *17*(2), 212–227. https://doi.org/10.1093/jcsl/krs014

Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford Academic.

Cornish, P. (Ed.) (2021). *The Oxford Handbook of Cyber Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.001.0001
Dean, S. E. (2013). Cyber Defense: securing military systems and critical civilian infrastructure from an electronic. *HRISQ*, *XIII*(3), 911.
Denardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No off Switch*. Yale University Press. https://doi.org/10.2307/j.ctvt1sgc0
Droege, C. (2012). Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. *International Review of the Red Cross*, *94*(886), 533–578. https://doi.org/10.1017/s1816383113000246
Dwan, J. H., Paige, T. P., & McLaughlin, R. (2022). Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers? *Law, Technology and Humans*, *3*, 52. https://doi.org/10.5204/lthj.1583
Etzioni, A., & Rice, C. J. (2015). *Privacy in a Cyber Age*. Springer. https://doi.org/10.1057/9781137513960
Faga, H. P. (2017). The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century. *Baltic Journal of Law & Politics*, *10*, 27. https://doi.org/10.1515/bjlp-2017-0001
Friis, K., & Ringsmose, J. (Eds.) (2016). *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*. Routledge & CRC Press. https://doi.org/10.4324/9781315669878
Frowe, H. (2022). *The Ethics of War and Peace: An Introduction*. Routledge/Taylor & Francis Group. https://doi.org/10.4324/9781003275466
Gheciu, A., & Wohlforth, W. C. (2018). *The Oxford Handbook of International Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198777854.001.0001
Gow, J., Dijxhoorn, E., Clare Kerr, R., & Verdirame, G. (Eds.) (2019). *Routledge Handbook of War, Law and Technology*. Routledge Taylor & Francis Group. https://doi.org/10.4324/9781315111759
Harrison Dinniss, H. (2012). *Cyber Warfare and the Laws of War*. Cambridge University Press. https://doi.org/10.1017/cbo9780511894527
Henriksen, A. (2019). The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity*, *5*(1), 3. https://doi.org/10.1093/cybsec/tyy009
Hollis, D. B., & Finnemore, M. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*, *110*(3), 425–479. https://doi.org/10.1017/s0002930000016894
Holt, T., Bossler, A., & Seigfried-Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge. https://doi.org/10.4324/9781315777870
Joyner, C. C. (2011). United States foreign policy interests in the Antarctic. *The Polar Journal*, *1*(1), 17–35. https://doi.org/10.1080/2154896x.2011.569384
Katagiri, N. (2021). Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab009
Klimburg, A. (2018). *The Darkening Web: The War for Cyberspace*. Penguin Books.
Knowles, J., & Thomas, P. A. (2016). *Effective Legal Research*. Sweet & Maxwell.
Kulesza, J., & Balleste, R. (2015). *Cybersecurity and Human Rights in the Age of Cyberveillance*. Rowman & Littlefield.
Levite, A., & Perkovich, G. (2017). Understanding cyber conflict. Georgetown University Press. https://doi.org/10.1353/book62546
Lewis, D. A., Modirzadeh, N. K., & Blum, G. (2019). Quantum of Silence: Inaction and Jus Ad Bellum. *Harvard Law School Program on International Law and Armed Conflict*. https://doi.org/10.54813/azzk2231
Lewis, J. A. (2018). Rethinking Cybersecurity: Strategy, Mass Effect, and States. Center for Strategic & International Studies; Rowman & Littlefield.
Liivoja, R., & Väljataga, A. (Eds.) (2021). *Autonomous Cyber Capabilities under International Law*. NATO Cooperative Cyber Defence Centre Of Excellence 2021.
Lucas, G. (2016). *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190276522.001.0001
Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, *21*(3), 405–428. https://doi.org/10.1093/jcsl/krw014
Mazanec, B. M. (2015). *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. University of Nebraska Press. https://doi.org/10.2307/j.ctt1d989jr
Mihr, A. (2017). *Cyber Justice : Human Rights and Good Governance for the Internet*. Springer.
Mihr, A. (2016). Cyber justice: cyber governance through human rights and a rule of law in the Internet. *US-China Law Review*, *13*(4). https://doi.org/10.17265/1548-6605/2016.04.002

Nissenbaum, D. (2015). *A Street Divided : Stories from Jerusalem's Alley of God*. St Martin's Press.
Ohlin, J. D., Govern, K., & Finkelstein, C. (Eds.) (2015). *Cyber War: Law and Ethics for Virtual Conflicts*. Oxford University Press.
Ossoff, W. (2021). Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace. *Harvard International Law Journal*, *62*(1), 298.
Putman, W. H., & Albright, J. R. (2018). *Legal Research, Analysis, and Writing*. Cengage Learning.
Roscini, M. (2010). World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law Online*, *14*(1), 85–130 https://doi.org/10.1163/18757413-90000050
Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
Schmitt, M. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*, *56*, 569.
Schmitt, M. (2012). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*, *54*, 13–37.
Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, *37*, 1998–1999.
Schmitt, M. N. (2012). "Attack" as a Term of Art in International Law: The Cyber Operations Context. In *4th International Conference on Cyber Conflict (CYCON 2012)*, Tallinn, Estonia (pp. 1–11).
Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288
Schmitt, M. N. (2014). Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, *54*, 698.
Schneier, B. (2013). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Springer.
Shackelford, S. J. (2012). Toward Cyber Peace: Managing Cyber Attacks through Polycentric Governance. *American University Law Review*. https://doi.org/10.2139/ssrn.2132526
Shackelford, S. J. (2014). Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press. https://doi.org/10.1017/cbo9781139021838
Shane, P. M., & Hunker, J. A. (Eds.) (2013). Cybersecurity : Shared Risks, Shared Responsibilities. Carolina Academic Press.
Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know®. Oxford University Press. https://doi.org/10.1093/wentk/9780199918096.001.0001
Travis, P. (2016). We're Going to Nicaragua: The United States, Nicaragua, and Counterterrorism in Central America during the 1980s. *Journal of Terrorism Research*, *7*, 38. https://doi.org/10.15664/jtr.1217
Tsagourias, N. (2012). The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II — the Use of Force. In *Yearbook of International Humanitarian Law* (Vol. 15, pp. 19–43). https://doi.org/10.1007/978-90-6704-924-5_2
Tsagourias, N., & Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, *31*(3), 941–967. https://doi.org/10.1093/ejil/chaa057
Tyler, T. R. (2017). Methodology in Legal Research. *Utrecht Law Review*, *13*(3), 130–141. https://doi.org/10.18352/ulr.410
Van Hoecke, M. (2011). *Methodologies of Legal Research*. Bloomsbury Publishing.
Wagner, B., Kettemann, M. C., & Vieth, K. (2019). *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations*. Edward Elgar Publishing. https://doi.org/10.4337/9781785367724
Watkins, D., & Burton, M. (2013). *Research Methods in Law*. Routledge. https://doi.org/10.4324/9780203489352
Watt, E. (2021). State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law. Elgar. https://doi.org/10.4337/9781789900101
Waxman, M. (2011). Cyber-Attacks as "Force" under UN Charter Article 2(4). *International Law Studies*, *43*.
Whyte, C., & Mazanec, B. (2018). *Understanding Cyber-Warfare: Politics, Policy and Strategy*. Routledge. https://doi.org/10.4324/9781315636504
Winterfeld, S., & Andress, J. (2013). *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Elsevier.
Wittes, B., & Blum, G. (2016). *The Future of Violence – Robots and Germs, Hackers and Drones*. Basic Books.
Wren, C. G., & Wren, J. R. (1986). *The Legal Research Manual: A Game Plan for Legal Research and Analysis* (2nd ed.). A-R Editions.
Yoo, C. S., & Blanchette, J.-F. (2015). *Regulating the Cloud*. MIT Press. https://doi.org/10.7551/mitpress/9780262029407.001.0001

Сведения об авторах

Мохаммад Минхазур Рахман – магистр права, преподаватель, кафедра права, Государственный университет Бангладеш
Адрес: Бангладеш, 1461, г. Дакка, Канчан, Саут Пурбачал
E-mail: sabitminhaz@gmail.com
ORCID ID: https://orcid.org/0009-0004-9764-5450

Тапос Кумар Дас – магистр права, доцент, кафедра права и юстиции, Джахангирнагарский университет; кандидат на соискание степени PhD, Школа права, Городской университет Гонконга
Адрес: Бангладеш, 1342, г. Дакка, Савар; Гонконг, Коулун, Коулун Тонг, Тат Чи Авеню, 83
E-mail: taposlaw@juniv.edu
ORCID ID: https://orcid.org/0000-0002-3349-8947

Вклад авторов

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

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 1 апреля 2024 г.
Дата одобрения после рецензирования – 18 апреля 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:341.4:004.8
EDN: https://elibrary.ru/nnftqi
DOI: https://doi.org/10.21202/jdtl.2024.46

Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming them

Mohammad Minhazur Rahman ✉
State University of Bangladesh, Dhaka, Bangladesh

Tapos Kumar Das
Jahangirnagar University, Dhaka, Bangladesh
City University of Hong Kong, Hong Kong

Keywords

cyberattack,
cybercrime,
digital technologies,
human rights,
international convention,
international law,
law,
legal liability,
principle of due diligence,
principle of proportionality,
principles of international law

Abstract

Objective: to categorize cyber attacks in the national and international legal sytems and to define legal measures to counter them at the international level.

Methods: include doctrinal legal analysis, formal legal, comparative legal methods, synthesis, induction, deduction, as well as methods of legal forecasting and modeling. International legal documents and acts of national legislation, judicial precedents, and doctrinal sources were studied.

Results: the article defines the legal consequences of cyberattacks, identifies difficulties in determining and holding individuals and organizations accountable for their commission, identifies national measures to counter cyberattacks based on the principle of proportionality, and systematizes the international legal framework for responding to cyberattacks. The main focus is on the urgent problems of identifying and verifying cyber weapons, establishing international standards for their use, developing methods of disarmament or limiting offensive cyber capabilities. The authors raise the issue of ensuring humanitarian activities, protecting critical infrastructure and the population through cybersecurity measures in wartime. The legal framework is analyzed; gaps and other defects are identified in the current regulation of exercising jurisdiction in such areas of cyber activity as international transactions, data localization and extraterritorial enforcement of national legislation. The parameters were developed and described within

✉ Corresponding author

which states may conduct proactive cyber operations to prevent or deter cyberattacks (cyber countermeasures). The main parameters are due diligence, legal decisions on using cyber countermeasures, proportionality of protection measures to the consequences of illegal actions.

Scientific novelty: this is due to the progressive solutions in the field of international legal regulation of cyber countermeasures by states responding to cybercrime. The solutions are formulated taking into account the impact of the countermeasures on human and civil rights and freedoms, including the right to privacy and freedom of speech.

Practical significance: the research results can be used to develop and improve international legal instruments in the field of combating cyberattacks and ensuring cybersecurity, and can serve as a model for national legislators when designing law-making solutions to counter cybercrime.

For citation

Rahman, M. M., & Das, T. K. (2024). Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming them. *Journal of Digital Technologies and Law, 2*(4), 973–1002. https://doi.org/10.21202/jdtl.2024.46

References

Andrew, J., & Bernard, F. (Eds.) (2021). *Human Rights Responsibilities in the Digital Age: States, Companies, and Individuals*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509938865

Bucci, S. (2018). Strategic Cyber Deterrence: The Active Cyber Defense Option by Scott Jasper. Rowman & Littlefield, 2017, 255 pp. *Strategic Studies Quarterly*, *12*(2), 134–135.

Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law*, *17*(2), 212–227. https://doi.org/10.1093/jcsl/krs014

Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford Academic.

Cornish, P. (Ed.) (2021). *The Oxford Handbook of Cyber Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.001.0001

Dean, S. E. (2013). Cyber Defense: securing military systems and critical civilian infrastructure from an electronic. *HRISQ*, *XIII*(3), 911.

Denardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No off Switch*. Yale University Press. https://doi.org/10.2307/j.ctvt1sgc0

Droege, C. (2012). Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. *International Review of the Red Cross*, *94*(886), 533–578. https://doi.org/10.1017/s1816383113000246

Dwan, J. H., Paige, T. P., & McLaughlin, R. (2022). Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers? *Law, Technology and Humans*, *3*, 52. https://doi.org/10.5204/lthj.1583

Etzioni, A., & Rice, C. J. (2015). *Privacy in a Cyber Age*. Springer. https://doi.org/10.1057/9781137513960

Faga, H. P. (2017). The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century. *Baltic Journal of Law & Politics*, *10*, 27. https://doi.org/10.1515/bjlp-2017-0001

Friis, K., & Ringsmose, J. (Eds.) (2016). *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*. Routledge & CRC Press. https://doi.org/10.4324/9781315669878

Frowe, H. (2022). *The Ethics of War and Peace: An Introduction*. Routledge/Taylor & Francis Group. https://doi.org/10.4324/9781003275466

Gheciu, A., & Wohlforth, W. C. (2018). *The Oxford Handbook of International Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198777854.001.0001

Gow, J., Dijxhoorn, E., Clare Kerr, R., & Verdirame, G. (Eds.) (2019). *Routledge Handbook of War, Law and Technology*. Routledge Taylor & Francis Group. https://doi.org/10.4324/9781315111759

Harrison Dinniss, H. (2012). *Cyber Warfare and the Laws of War*. Cambridge University Press. https://doi.org/10.1017/cbo9780511894527
Henriksen, A. (2019). The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity*, *5*(1), 3. https://doi.org/10.1093/cybsec/tyy009
Hollis, D. B., & Finnemore, M. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*, *110*(3), 425–479. https://doi.org/10.1017/s0002930000016894
Holt, T., Bossler, A., & Seigfried-Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge. https://doi.org/10.4324/9781315777870
Joyner, C. C. (2011). United States foreign policy interests in the Antarctic. *The Polar Journal*, *1*(1), 17–35. https://doi.org/10.1080/2154896x.2011.569384
Katagiri, N. (2021). Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab009
Klimburg, A. (2018). *The Darkening Web: The War for Cyberspace*. Penguin Books.
Knowles, J., & Thomas, P. A. (2016). *Effective Legal Research*. Sweet & Maxwell.
Kulesza, J., & Balleste, R. (2015). *Cybersecurity and Human Rights in the Age of Cyberveillance*. Rowman & Littlefield.
Levite, A., & Perkovich, G. (2017). Understanding cyber conflict. Georgetown University Press. https://doi.org/10.1353/book62546
Lewis, D. A., Modirzadeh, N. K., & Blum, G. (2019). Quantum of Silence: Inaction and Jus Ad Bellum. *Harvard Law School Program on International Law and Armed Conflict*. https://doi.org/10.54813/azzk2231
Lewis, J. A. (2018). Rethinking Cybersecurity: Strategy, Mass Effect, and States. Center for Strategic & International Studies; Rowman & Littlefield.
Liivoja, R., & Väljataga, A. (Eds.) (2021). *Autonomous Cyber Capabilities under International Law*. NATO Cooperative Cyber Defence Centre Of Excellence 2021.
Lucas, G. (2016). *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190276522.001.0001
Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, *21*(3), 405–428. https://doi.org/10.1093/jcsl/krw014
Mazanec, B. M. (2015). *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. University of Nebraska Press. https://doi.org/10.2307/j.ctt1d989jr
Mihr, A. (2017). *Cyber Justice : Human Rights and Good Governance for the Internet*. Springer.
Mihr, A. (2016). Cyber justice: cyber governance through human rights and a rule of law in the Internet. *US-China Law Review*, *13*(4). https://doi.org/10.17265/1548-6605/2016.04.002
Nissenbaum, D. (2015). *A Street Divided : Stories from Jerusalem's Alley of God*. St Martin's Press.
Ohlin, J. D., Govern, K., & Finkelstein, C. (Eds.) (2015). *Cyber War: Law and Ethics for Virtual Conflicts*. Oxford University Press.
Ossoff, W. (2021). Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace. *Harvard International Law Journal*, *62*(1), 298.
Putman, W. H., & Albright, J. R. (2018). *Legal Research, Analysis, and Writing*. Cengage Learning.
Roscini, M. (2010). World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law Online*, *14*(1), 85–130 https://doi.org/10.1163/18757413-90000050
Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
Schmitt, M. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*, *56*, 569.
Schmitt, M. (2012). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*, *54*, 13–37.
Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, *37*, 1998–1999.
Schmitt, M. N. (2012). "Attack" as a Term of Art in International Law: The Cyber Operations Context. In *4th International Conference on Cyber Conflict (CYCON 2012)*, Tallinn, Estonia (pp. 1–11).
Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288
Schmitt, M. N. (2014). Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, *54*, 698.
Schneier, B. (2013). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Springer.

Shackelford, S. J. (2012). Toward Cyber Peace: Managing Cyber Attacks through Polycentric Governance. *American University Law Review*. https://doi.org/10.2139/ssrn.2132526

Shackelford, S. J. (2014). Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press. https://doi.org/10.1017/cbo9781139021838

Shane, P. M., & Hunker, J. A. (Eds.) (2013). Cybersecurity : Shared Risks, Shared Responsibilities. Carolina Academic Press.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know®. Oxford University Press. https://doi.org/10.1093/wentk/9780199918096.001.0001

Travis, P. (2016). We're Going to Nicaragua: The United States, Nicaragua, and Counterterrorism in Central America during the 1980s. *Journal of Terrorism Research*, *7*, 38. https://doi.org/10.15664/jtr.1217

Tsagourias, N. (2012). The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II — the Use of Force. In *Yearbook of International Humanitarian Law* (Vol. 15, pp. 19–43). https://doi.org/10.1007/978-90-6704-924-5_2

Tsagourias, N., & Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, *31*(3), 941–967. https://doi.org/10.1093/ejil/chaa057

Tyler, T. R. (2017). Methodology in Legal Research. *Utrecht Law Review*, *13*(3), 130–141. https://doi.org/10.18352/ulr.410

Van Hoecke, M. (2011). *Methodologies of Legal Research*. Bloomsbury Publishing.

Wagner, B., Kettemann, M. C., & Vieth, K. (2019). *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations*. Edward Elgar Publishing. https://doi.org/10.4337/9781785367724

Watkins, D., & Burton, M. (2013). *Research Methods in Law*. Routledge. https://doi.org/10.4324/9780203489352

Watt, E. (2021). State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law. Elgar. https://doi.org/10.4337/9781789900101

Waxman, M. (2011). Cyber-Attacks as "Force" under UN Charter Article 2(4). *International Law Studies*, *43*.

Whyte, C., & Mazanec, B. (2018). *Understanding Cyber-Warfare: Politics, Policy and Strategy*. Routledge. https://doi.org/10.4324/9781315636504

Winterfeld, S., & Andress, J. (2013). *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice.* Elsevier.

Wittes, B., & Blum, G. (2016). *The Future of Violence – Robots and Germs, Hackers and Drones*. Basic Books.

Wren, C. G., & Wren, J. R. (1986). *The Legal Research Manual: A Game Plan for Legal Research and Analysis* (2nd ed.). A-R Editions.

Yoo, C. S., & Blanchette, J.-F. (2015). *Regulating the Cloud*. MIT Press. https://doi.org/10.7551/mitpress/9780262029407.001.0001

Authors information

Mohammad Minhazur Rahman – LLM, Lecturer, Department of Law, State University of Bangladesh
Address: South Purbachal, Kanchan, Dhaka-1461, Bangladesh
E-mail: sabitminhaz@gmail.com
ORCID ID: https://orcid.org/0009-0004-9764-5450

Tapos Kumar Das – LLM, Associate Professor, Department of Law & Justice, Jahangirnagar University; PhD Student, School of Law, City University of Hong Kong
Address: Savar, Dhaka-1342, Bangladesh; 83 Tat Chee Avenue, Kowloon Tong, Kowloon, Hong Kong
E-mail: taposlaw@juniv.edu
ORCID ID: https://orcid.org/0000-0002-3349-8947

Authors' contributions

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

Conflict of interests

The authors declare no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

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

Article history

Date of receipt – April 1, 2024
Date of approval – April 18, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024