УДК 341 DOI: 10.31249/iajpravo/2025.02.13

ЗАХАРОВ Т.В.[1] МЕЖДУНАРОДНО-ПРАВОВОЕ ИЗМЕРЕНИЕ СОВРЕМЕННОГО РАЗВИТИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ (Обзор)

Аннотация. В обзоре представлены позиции зарубежных ученых по отдельным вопросам влияния международного права на использование информационно-коммуникационных технологий (ИКТ). Рассматривается проблема развития международного права в области использования ИКТ с позиции международной безопасности. Освещена концепция «промежуточного состояния» (между состояниями «войны» и «мира») взаимодействия государств в информационном пространстве, концепция «информационной атаки» в военно-правовой доктрине США.

Ключевые слова: международное право; международная безопасность; информационно-коммуникационные технологии (ИКТ); кибератака.

ZAKHAROV T.V. The International Legal Dimension of the Modern Development of Information and Communication Technologies (Review)

Abstract. The review presents the positions of foreign scientists on certain issues of the influence of international law on the use of information and communication technologies (ICT). The problem of the development of international law in the field of the use of ICT from the perspective of international security is considered. The article highlights the concept of an “intermediate state” (between states of “war” and “peace”) of interaction between states in the information space, the concept of an “information attack” in the military-legal doctrine of the United States.

[1] *Захаров Тимофей Владимирович*, научный сотрудник отдела правоведения ИНИОН РАН.

Keywords: international law; international security; information and communication technologies (ICT); cyberattack.

Для цитирования: Захаров Т.В. Международно-правовое измерение современного развития информационно-коммуникационных технологий (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2025. – № 2. – С. 156–166. – DOI: 10.31249/iajpravo/2025.02.13

Введение

Динамика развития информационно-коммуникационных технологий (ИКТ) значительно опередила правовое регулирование складывающихся в связи с этим общественных отношений. Это создало условия для образования серых зон, когда определенное использование ИКТ потенциально является противоправным. Проблема обостряется широким использованием ИКТ в военных целях. В связи с этим ученые поднимают сложные вопросы международно-правового регулирования, развития международного права в данной области.

Международно-правовые основы использования ИКТ в контексте международной безопасности. Х.А. Балуджи – независимый исследователь, занимающийся вопросами международной безопасности, рассматривает в своей статье международно-правовые основы использования ИКТ в контексте международной безопасности. В статье делается акцент на проблемах, связанных с технологическими решениями международной безопасности.

За более чем два десятилетия дискуссий в ООН по вопросу информационно-коммуникационных технологий (ИКТ) в контексте международной безопасности так и не удалось прийти к какому-либо окончательному решению. Стороны, отстаивающие конкурирующие подходы, продолжают споры. В данном вопросе основная проблема сводится к разработке юридически обязывающего документа в области ИКТ в контексте международной безопасности [1, с. 90].

При обращении к данной проблеме, автор предлагает рассмотреть и использовать три актуальных, по его мнению, допущения: 1) человеческая жизнь имеет как материальное, так и нематериальное измерение. С учетом существующих реалий «мы, – полагает автор, – не можем считать физическую безопасность важнее, чем безопасность в сфере ИКТ. Количество ИКТ-инци-

дентов, в том числе хакерство, фишинг и тому подобное, по всему миру исчисляется миллиардами. Более того, последствия некоторых из нападений с использованием ИКТ, которые направлены на правительства или касаются национальных активов и богатства страны, носят более серьезный характер и сопоставимы с физическими нападениями, например, с использованием военной техники» [1, с. 91]; 2) операции с использованием ИКТ могут привести к физическим разрушениям и увечьям. Кроме того, использование ИКТ несет в себе значительную опасность в плане вмешательства в деятельность, подрыва и возможного уничтожения ядерных объектов, поставить под угрозу целостность и эффективность систем управления и контроля над ядерными объектами [там же, с. 91–92]; 3) заявленная государствами цель в многосторонних переговорах по вопросам международных документов в физическом и нефизическом измерениях – укрепление международного мира и безопасности путем предотвращения применения силы и угрозы силой, уважение суверенного равенства государств, мирное урегулирование международных споров и отказ от вмешательства во внутренние дела друг друга. Противодействие развитию международного права в любой из этих областей может стать проверкой реальной политической воли государств [там же, с. 92].

Вопросы международного права, включая нормы, правила и принципы безопасности в сфере ИКТ, широко отражены в дискуссиях, докладах и итоговых документах Рабочей группы открытого состава (РГОС) ООН и различных групп правительственных экспертов (ГПЭ) в области ИКТ в контексте международной безопасности. Ряд развитых западных стран прямо выступают против развития международного права в этой области – по крайней мере в настоящее время – и подчеркивает достаточность существующих норм международного права для обеспечения безопасного и стабильного ИКТ-пространства [там же, с. 92].

По мнению группы других стран, в основном развивающихся, а также России и Китая, – существующих норм международного права недостаточно для достижения цели обеспечения международного мира и безопасности в ИКТ-пространстве. В связи с этим для достижения желаемого уровня безопасности в этой области следует пересмотреть рекомендованные ГПЭ нормы и, помимо этого, разработать и применять юридически обязывающий документ в качестве международного договора или конвенции [там же, с. 93].

По мнению Х.А. Балуджи, «крайне важно обеспечить, чтобы в основе выводов лежали технические, а не политические мотивы. Таким образом, мир сможет вести борьбу с угрозами ИКТ, характер которых постоянно меняется» [1, с. 96].

Итоги переговорных процессов в рамках РГОС и других соответствующих международных форумов, включая Первый комитет Генеральной Ассамблеи ООН, свидетельствуют о том, что некоторые страны прилагают усилия для изложения своих взглядов и позиций в письменной и устной формах, однако все эти действия объединяет один общий аспект: участвующие в переговорах делегаты объединяются политически в соответствии с позицией своих правительств. В рамках этого подхода страны, принимающие решения по собственной воле и согласию, не обязаны обосновывать свою позицию. Однако ожидается, что правительства и делегации будут рассматривать необходимые рамочные основы и рациональные, логические и правовые причины, чтобы убедить других в рамках многосторонней дипломатии. Обращение к беспристрастным международным экспертам и принятие представленного ими решения поможет выйти из тупиковой ситуации. В связи с этим вопрос может быть передан на рассмотрение Комиссии международного права [там же].

Среди других вариантов рассматривается возможность проведения специальной сессии РГОС по международному праву и нормам непосредственно для решения этого вопроса. К участию в работе сессии возможно было бы привлечь экспертов в области права из разных стран. Полезным для обеспечения всестороннего понимания соответствующих правовых аспектов стало бы, по мнению (Х.А. Балуджи, обращение за юридической консультацией в специализированный правовой орган, обладающий опытом в области ИКТ в контексте международной безопасности [там же].

Ценным подспорьем и ориентиром, с точки зрения Х.А. Балуджи, будет задействование внутреннего экспертного опыта в лице юрисконсультов, правоведов и экспертов в области связанного с ИКТ права. Их мнение поможет пролить свет на правовые последствия и возможные решения, что позволит обеспечить соблюдение норм международного права при одновременном содействии развитию сферы ИКТ в контексте международной безопасности для всех. Другой подход заключается в проведении взаимной экспертной оценки (peer review), в ходе которой специалисты в области права из разных стран и с разным опытом подвергают вопрос критическому анализу, представляют свои мнения и

предлагают рекомендации. Такая совместная работа может способствовать выявлению пробелов и несоответствий в том, что касается юридического толкования, и проведению комплексного обсуждения [1, с. 96–97].

Наконец, на основе консультативного правового заключения, полученного с помощью этих различных каналов, возможно прояснить правовые вопросы и найти практические решения, соответствующие нормам международного права. Конечная цель состоит в том, чтобы направить государства-члены на путь к принятию деполитизированного и непредвзятого технического решения и преодолеть сложившуюся безвыходную ситуацию. Однако в заключении, Х.А. Балуджи, обращает внимание на необходимость тщательного изучения имеющихся пробелов в понимании и их восполнения с помощью формализованного и юридически обязывающего соглашения. В отсутствие таких мер нынешнее состояние неопределенности может так и не выйти за рамки простого толкования, не имеющего юридической силы. С тем чтобы добиться ясности и исполнения обязательств, необходимо, считает он, выработать систему положений, которая бы закрепила и придала законную силу этому пониманию в юридически обязательной форме [там же].

Регулирование роли киберпространства с помощью международного права Д. Джованелли, исследователь права в Центре передового опыта НАТО по совместной киберзащите (NATO cooperative cyber defence centre of excellence) (Эстония) представляет оппонирующий предыдущему автору подход, рассматривая особенности правовых состояний взаимодействия государств в киберпространстве. Отсутствие общего понимания того, как международное право применяется к ИКТ, вызвано некоторыми фундаментальными пробелами в международном праве, а не отсутствием юридических норм, относящихся к конкретной предметной области, считает Д. Джованелли [3, p. 3].

Чтобы дать определение отношениям между Соединенными Штатами и Советским Союзом во время холодной войны, Филип К. Джессап, цитирует которого Д. Джованелли, предложил возможность преодолеть традиционную дихотомию между «войной» и «миром» и рассмотреть «промежуточное состояние», которое не является ни тем, ни другим. В таком промежуточном состоянии было бы признано, что враждебные стороны могут участвовать в действиях, которые не были бы мирными и все же были бы далеки от того, что сейчас удобно называть тотальной войной [ibid., p. 2–3].

Из-за правовой неопределенности того, как международное право применяется к использованию ИКТ, создались условия для подобного промежуточного состояния в киберпространстве. Нынешний ландшафт глобальной безопасности характеризуется «постоянными военными действиями низкой интенсивности», которые основные действующие лица часто полностью отрицают [3, p. 3]. Государства с разным геополитическим положением, к примеру Россия, Япония и Бразилия, выразили обеспокоенность активным участием в кибероперациях гражданских лиц. Возникла необходимость уточнения понятия прямого участия комбатантов и гражданских лиц в военных действиях с применением ИКТ. Международный порядок, основанный на правилах, предполагает, что государства – в силу своей демократической легитимности – должны сохранять монополию на применение силы, говорит автор [ibid., p. 4].

Обеспокоенность государств участием гражданских лиц в кибератаках представляется обоснованным в свете двух взаимосвязанных факторов: (I) обязанности государства проявлять должную осмотрительность и не допускать использования своей территории для злонамеренной кибердеятельности, и (II) того факта, что Россия публично привлекает внимание к кибератакам, исходящим от стран-членов НАТО [ibid., p. 8].

Один из основных принципов международного гуманитарного права, когда стороны, участвующие в конфликте, должны проводить различие между гражданским населением и непосредственными участниками военных действий (комбатантами) для обеспечения защиты гражданского населения и гражданских объектов, неприменим к состоянию мирного времени. Из этого складывается положение, когда государства, пользуясь промежуточным состоянием, могут широко использовать гражданскую инфраструктуру и гражданских лиц в проведении кибероперациях, в том числе сопоставимых с применением силы. Можно было бы предположить, пишет Д. Джованелли, что в промежутке между «чистым» миром и «тотальной» войной государства могут постоянно вступать в борьбу друг с другом за власть и другие ценности, используя все инструменты политики, в разной степени принудительные методы, варьирующиеся от наименее интенсивных до наиболее интенсивных. Однако нынешние конфликты в киберпространстве отличаются от прошлых примеров ограниченного применения силы, поскольку они носят постоянный и непрекращающийся характер (временно́й элемент) и их масштабы не

ограничены конкретной географической областью (пространственный элемент) [3, p. 8].

Ведя перманентную кибервойну низкой интенсивности, государства проявляют своего рода враждебность к воюющим, по крайней мере, с качественной – хотя и не количественной – точки зрения. Таким образом, принцип различия между гражданским населением и комбатантами в киберпространстве, по мнению автора, следует толковать шире. В киберпространстве необходимо учитывать не только состояние вооруженного конфликта, но и промежуточные состояния [ibid., p. 9].

Д. Джованелли выделяет ряд трудностей в толковании международного права, применимого к использованию ИКТ в противостояниях государств. Более сложными в понимании становятся такие понятия международного гуманитарного права, как «прямое участие в военных действиях» «применение силы в киберпространстве». Узкое толкование понятия «объект нападения» может способствовать формированию политического и общественного мнения о том, что кибероперации наносят меньший ущерб, чем традиционные боевые операции. Разграничение разведывательных и военных операций в киберпространстве является весьма сложным, поскольку часто одно и то же вредоносное программное обеспечение может использоваться как для хищения данных, шпионажа, так и для причинения ущерба [ibid., p. 9–13].

Не вполне понятным остается действие права на самооборону в соответствии со ст. 51 Устава ООН – традиционно она ограничивается случаями вооруженного нападения, т.е. наиболее серьезными формами применения силы [ibid., p. 11]. Очевидно, что в случае кибероперации, уровень которых ниже порога применения силы, сдерживание может быть достигнуто главным образом за счет принятия контрмер, включая, в частности, контрмеры, принимаемые потерпевшими государствами или от имени потерпевшего государства (коллективные контрмеры) [ibid., p. 15]. Тем не менее, возвращаясь к сложности определения понятия «применение силы в киберпространстве», нельзя не видеть, что противостояние государств в киберпространстве ведется средствами, характерными для военного времени [ibid., p. 43]. В соответствии с проектами статей об ответственности государств за международно-противоправные деяния 2001 г. контрмеры не затрагивают обязательства воздерживаться от угрозы силой или ее применения, закрепленного в Уставе ООН [ibid., p. 11].

Отдельную проблему представляет признание ответственности государств за действия негосударственных субъектов. При недоказанности эффективного контроля государством действий частных лиц, тайные операции по финансовой поддержке, обучению или поставкам оружия, разведывательных данных и материально-технической поддержке негосударственных субъектов, могут быть истолкованы как нарушение принципа невмешательства, а не нарушение запрета на угрозу силой или ее применение [3, p. 13].

Военно-правовая доктрина США и формирующаяся киберсреда военного времени. Э. Бобенрит, судья-адвокат армии США, профессор права национальной безопасности в правовом центре и школе права в Шарлоттсвилле (США) и С. Уоттс, профессор Военной академии США Вест-Пойнт, соредактор журнала «Lieber Studies Series» (Oxford University Press) (Великобритания), рассматривают использование ИКТ в вооруженных конфликтах, изменения в концепции ведения боевых действий в киберпространстве США [2].

Подход США к войне ближайшего будущего предусматривает интеграцию кибероперациий практически во все виды деятельности на поле боя. В пределах разрабатываемой Пентагоном концепции «многодоменные операции» предполагается полное объединение боевых возможностей и направлений действий военных подразделений, включая кибероперации, в единую и взаимоподдерживающую систему наведения на цель [ibid., p. 3].

Однако применяемая в США нормативно-правовая основа для проведения кибероперациий в военное время ограничена. Это особенно верно в отношении норм военного права, применимых к операциям, которые характеризуются как находящиеся ниже установленного правом порога признания ее атакой, составляющим значительную часть кибероперациий во время вооруженных конфликтов [ibid., p. 4]. Применение же прогрессивных, авангардных правовых подходов к реальным операциям сложно и сопряжено с массой трудностей. «Часто неясно, – пишут авторы, – в какой степени прогрессивные теоретические концепции отражают lex lata в понимании государств. Тем не менее обзор новых концепций ведения кибервойн в сопоставлении с правовыми рекомендациями, разработанными почти десять лет назад, ясно показывает необходимость обновления доктрины киберправа военного времени, считают авторы [ibid., p. 4].

В 2023 г. Департамент вооруженных сил США опубликовал внутреннюю инструкцию под неопределенным названием «Ин-

формация», в которой приведены важные правила, касающиеся использования ИКТ в военных действиях. Инструкция переводит ИКТ из их прежнего статуса вспомогательных средств, применяемых в конфликте, в статус самостоятельной функции ведения боевых действий. Дается указание армейским командирам учитывать возможности ИКТ и последствия их использования, использовать ИКТ в сочетании с физическими средствами с целью повлиять на восприятие угроз противником, на его способность осуществлять командование своими силами [2, p. 7].

Внимание привлекает рассмотрение в данной инструкции «атаки», как информационной деятельности. В стремлении к информационному преимуществу, действия должны быть «ориентированы на наступление». Это, в частности, предполагает захват и удержание инициативы в отношении информационной активности противника, быстрые действия против информационных платформ противника и быструю адаптацию, чтобы лишить силы противника потенциальных информационных преимуществ. На каждом шагу эта новая доктрина заставляет командиров воспринимать информацию как часть боевой мощи, а не как вспомогательное средство. Информация – неотъемлемая часть общего арсенала средств разрушения и дезорганизующей силы, которые военное подразделение может применить против противника. Это, в свою очередь, предписывает вооруженным силам использовать все соответствующие возможности для атаки на данные, информацию и сети, представляющие угрозу [ibid.].

Инструкция Министерства обороны США «Информация в рамках совместных операциях» 2022 г. также закрепляет широкое понимания ИКТ в военных действиях. Она определяет информационную мощь как способность проявлять свою волю посредством распространения, эксплуатации, отрицания и сохранения информации. Инструкция удивительно откровенно, хотя, несомненно, точно оценивает смартфоны, сеть Интернет и социальные сети как информационные платформы, имеющие отношение к ведению боевых действий [2, p. 8].

И в инструкции Департамента вооруженных сил США, и в инструкции Министерства обороны США предполагается, что потенциальные противники США относятся к информации аналогичным образом [ibid.].

Приоритетными направлениями атаки являются блокирование, дезорганизация, уничтожение или манипулирование широким спектром киберсистем противника и систем технологий, основан-

ных на электромагнитном спектре, а также данными, которые они хранят и передают. Ожидаемые военные преимущества этих атак включают в себя ослабление командования и контроля противника, снижение его собственных возможностей в области ведения информационной войны [2, p. 8].

Формируемая США доктрина информационных атак делает акцент на воздействии, а не на разрушении ради него самого, говорят авторы. Цели могут быть выбраны не в соответствии с их природой, а скорее в соответствии с тем, как противник использует или может использовать их. Доктрина информационных атак определяет разведку киберпространства, использование социальных сетей и сбор общедоступной информации как важные источники военного преимущества противника, лишение или подрыв которых приводит к значительным военным результатам [ibid.].

Заключение

Отчеты о кибератаках, публикуемые государствами, как отмечает Э. Бобенрит и С. Уоттс) разнятся настолько, что не дают четкого понимания сегодняшних конфликтов в киберпространстве. Очевидной стала конкуренция в киберпространстве между Соединенными Штатами и Китаем и Россией [3, p. 3–4]. В то же время, в отличие от холодной войны, киберконкуренция ведется с использованием средств и возможностей, неотличимые от тех, которые были бы характерны для военного времени [ibid., p. 43].

По мере того как возможности в киберпространстве расширяются и все больше интегрируются в оперативные средства военных подразделений, преимущества четкой правовой позиции по поднимаемым вопросам, с точки зрения Э. Бобенрит и С. Уоттс, будет служить многим стратегическим, дипломатическим и юридическим интересам государства и международной правовой системы в целом [2, p. 4].

Юридически обязывающее соглашение могло бы способствовать укреплению доверия стран, сдерживанию нападений с использованием ИКТ и созданию более безопасной цифровой среды [1, с. 95].

Список литературы

1. Балуджи Х. Вопрос международного права, а также норм, правил и принципов в сфере информационно-коммуникационных технологий в контексте ме-

ждународной безопасности: проблемы и анализ // Международная жизнь. – 2024. – Февраль. – С. 90–97.
2. Bobenrieth E., Watts S. US Military Legal Doctrine and the Emerging Wartime Cyber Environment // International Review of the Red Cross. – Cambridge, 2024. – First view. – P. 1–24.
3. Giovannelli D. Handling Cyberspace's State of Intermediacy Through Existing International Law // International Review of the Red Cross. – Cambridge, 2024. – First view. – P. 1–44.