Vestnik RUDN. International Relations. ISSN 2313-0660 (Print), ISSN 2313-0679 (Online)
Вестник РУДН. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ
2025 Vol. 25 No. 1 67–77
http://journals.rudn.ru/international-relations

DOI: 10.22363/2313-0660-2025-25-1-67-77
EDN: KACFAB

Научная статья / Research article

Разграничение гражданских и военных объектов в условиях развития информационно-коммуникационных технологий в ходе вооруженных конфликтов

Я.Н. Аду[1,2,3] ✉, **М.С. Рамич**[1]

[1]Российский университет дружбы народов, Москва, Российская Федерация
[2]Оренбургский государственный университет, Оренбург, Российская Федерация
[3]Уральский государственный экономический университет, Екатеринбург, Российская Федерация
✉ adu-ya@rudn.ru

Аннотация. Поражение разных объектов как гражданского, так и военного назначения в современных вооруженных конфликтах реанимирует дискуссию о разграничении гражданских и военных объектов в действующих международных инструментах в международном гуманитарном праве (МГП). В современных реалиях, с одной стороны, наличие тяжелой артиллерии не является преимуществом без современных информационно-коммуникационных технологий (ИКТ), которые могут обеспечить превосходство одной из сторон конфликта, в частности в контексте концепции сетецентричных войн, подразумевающих единую систему управления войсками, эффективное использование спутников для выявления дислокации войск противника и т. д. С другой стороны, информационное пространство стало полноценным театром военных действий, где проводятся информационные и кибероперации, направленные на снижение боевого духа противника, создание социальной напряженности и парализацию работы критически важных информационных ресурсов. Наличие продвинутых систем связи, Интернета и спутниковых данных является безусловным преимуществом в современных конфликтах, но осложняет разграничение характеристик гражданского и военного объекта, особенно в условиях, когда один и тот же объект может служить для гражданских и военных целей. Цель исследования — проанализировать трудности, возникшие в определении гражданского объекта в контексте развития информационно-коммуникационных технологий в связи с их двойным использованием как в гражданских, так и в военных целях применительно к современным конфликтам. Авторы приходят к выводу, что определение гражданского объекта, как представляется в МГП, усложняется в условиях развития информационно-телекоммуникационных технологий ввиду своего двойного назначения. Несмотря на то, что современные положения международного права защищают гражданские объекты, развитие ИКТ «размывает» критерии их определения в условиях современных вооруженных конфликтов.

Ключевые слова: международное гуманитарное право, комплексная инфраструктура информационно-коммуникационных технологий, объекты двойного назначения, Женевские конвенции 1949 года

Заявление о конфликте интересов. Авторы заявляют об отсутствии конфликта интересов.
Вклад авторов. Авторы внесли равнозначный вклад в разработку дизайна, проведение исследования и подготовку текста статьи.

Для цитирования: *Аду Я. Н., Рамич М. С.* Разграничение гражданских и военных объектов в условиях развития информационно-коммуникационных технологий в ходе вооруженных конфликтов // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2025. Т. 25, № 1. С. 67–77. https://doi.org/10.22363/2313-0660-2025-25-1-67-77

The Principle of Distinction Between Civilian Objects and Military Objectives in the Context of the Development of Information and Communication Technologies in Armed Conflicts

Yao N. Adu[1,2,3] ✉, Mirzet S. Ramich[1]

[1]RUDN University, Moscow, Russian Federation
[2]Orenburg State University, Orenburg, Russian Federation
[3]Ural State University of Economics, Ekaterinburg, Russian Federation
✉adu-ya@rudn.ru

Abstract. The destruction of infrastructure in modern armed conflicts, whether civilian or military, has led to renewed of interest in the discussion on the distinction between civilian objects and military objectives in the current international instruments of international humanitarian law (IHL). On the one hand, in contemporary realities, the presence of heavy artillery is not an advantage without modern information and communication technologies (ICT), which determine the benefits of the parties to the conflict, in particular in the context of the concept of network-centric warfare, which implies a unified system of troop control, the effective use of satellites to identify the dislocation of enemy troops, etc. On the other hand, the information space has become a full-fledged battlefield, where information and cyber operations are conducted to reduce the enemy's morale, create social tension, and paralyze the operation of critical information resources. The availability of advanced communication systems, the Internet, and satellite data is an undoubted advantage in modern warfare, which complicates the concepts of distinction between civilian objects and military objectives, especially when the same object can serve both civilian and military purposes. The purpose of this article is to analyze the complexities that have arisen in the definition of a civilian object in the context of the development of ICTs due to their dual use for both civilian and military purposes in relation to modern conflicts. As a result of the study, the authors conclude that the definitions of civilian objects, as outlined in IHL, become more complex in the context of the development of ICT given its dual purpose. The authors assume that despite the protective measures afforded by contemporary international law with regard to civilian objects, the development of ICTs "erodes" the criteria for their definition in modern armed conflicts.

Key words: international humanitarian law, integrated infrastructure of information and communication technologies, dual-use facilities, Geneva Conventions of 1949

Conflicts of interest. The authors declare no conflicts of interest.
Authors' contributions. The authors made an equal contribution to the design, research and preparation of the final article's text.

For citation: Adu, Y. N., & Ramich, M. S. (2025). The principle of distinction between civilian objects and military objectives in the context of the development of information and communication technologies in armed conflicts. *Vestnik RUDN. International Relations*, 25(1), 67–77. https://doi.org/10.22363/2313-0660-2025-25-1-67-77

Введение

Вопрос разграничения гражданских и военных объектов обсуждается учеными с момента принятия четырех Женевских конвенций 1949 г. и дополнительных Протоколов к ним в связи с тем, что данные инструменты не дают четкого определения гражданских объектов. Например, содержание ст. 52 дополнительного Протокола I определяет их абстрактно и не полностью. Вопрос правового статуса гражданского объекта, особенно при его двойном назначении, остается предметом рассмотрения и анализа российских и зарубежных ученых[1].

[1] См.: Тиунов О. И. Международное гуманитарное право : учебник. Москва : Изд-во Норма, 2023; Международное право : в 2 томах. Т. 2: Особенная часть : учебник для вузов. 2-е изд., перераб. и доп. / под ред.

Определение гражданского объекта осложняется применением современных информационно-коммуникационных технологий (ИКТ), представляющих комплексные военно-гражданские изобретения и инфраструктуру, в различных целях (как военных, так и гражданских).

Цель исследования — выявить последствия отсутствия четкого определения гражданского объекта в инструментах международного гуманитарного права (МГП) и трудности, возникающие при попытке решения данного вопроса, особенно в области ИКТ. Для достижения поставленной цели необходимо решить комплексные задачи: определить понятие гражданского объекта и его правовое значение в международном гуманитарном праве, проанализировать сложность разграничения гражданских и военных объектов, особенно в условиях развития ИКТ в связи с их двойным назначением, в том числе в гражданской и военной сферах, и определять ответственность воюющих сторон в условиях ведения войны.

Роль ИКТ в современных вооруженных конфликтах

С учетом комплексности правовой сферы регулирования МГП оно имеет ряд различных трактовок. В настоящее время наиболее распространенное определение международного гуманитарного права, которое применяется в российской учебной литературе, принадлежит российскому ученому-международнику О.И. Тиунову. По его мнению, «международное гуманитарное право представляет собой отрасль международного (публичного. — *Прим. авт.*) права, состоящую из совокупности международно-правовых принципов и норм, применяемых в условиях вооруженных конфликтов (международных и немеждународных), предусматривающих права и обязанности субъектов международного права и иных участников вооруженных конфликтов по соблюдению и обеспечению защиты жертв вооруженных конфликтов, гражданского населения, гражданских объектов и культурных ценностей, а также обязанности таких субъектов по запрещению применения определенных средств и методов введения вооруженных действий»[2].

Источники международного гуманитарного права состоят в основном из так называемых Гаагского права, Женевского права и иных международных правовых норм, принятых в этой области. Разработка и принятие норм Гаагского и Женевского права уходят корнями во вторую половину XVIII и начало XIX в., когда современные ИКТ еще не существовали или находились в стадии начала их разработки и развития.

Сегодня, спустя почти полвека после принятия трех дополнительных протоколов[3] к четырем Женевским конвенциям[4], произошел большой скачок развития в области ИКТ, невиданный в истории развития человеческого общества. И если в последние десятилетия удалось достичь серьезного прогресса в сфере средств ведения войны, например в области запретов на производство, накопление и распространение определенных видов оружия, таких как биологическое[5], бактериологическое[6], ядерное[7] и др., то другие, например гиперзвуковое или лазерное, вообще не регулируются или регулируются частично современным международным гуманитарным

А. Я. Капустина. Москва : Изд-во Юрайт, 2025. См. также: (Фуркало, 1982; Блищенко, 1984; Smith, 2002; Schmitt, 2008; Dinstein, 2012; Routledge Handbook…, 2016).

[2] Международное право : в 2 томах. Т. 2: Особенная часть : учебник для вузов. 2-е изд., перераб. и доп. / под ред. А. Я. Капустина. Москва : Изд-во Юрайт, 2025. С. 102.

[3] Geneva Conventions of 1949, Additional Protocols and Their Commentaries // International Humanitarian Law Databases. URL: https://ihl-databases.icrc.org/en/ihl-treaties/geneva-conventions-1949additional-protocols-and-their-commentaries (accessed: 30.11.2022).

[4] Ibid.

[5] Конвенция о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении // Организация Объединенных Наций. URL: https://www.un.org/ru/documents/decl_conv/conventions/bacweap.shtml (дата обращения: 30.11.2022).

[6] Там же.

[7] Договор о запрещении ядерного оружия // Организация Объединенных Наций. 07.07.2017. URL: https://docs.un.org/ru/A/CONF.229/2017/8 (дата обращения: 30.11.2022).

правом. То же самое можно сказать и о ИКТ, ставших важной частью военного потенциала ряда государств.

Дж. Най, сравнивая развитие киберпотенциала стран с ядерным оружием, делает предположение, что атаки из киберпространства, где затраты сравнительно низкие, могут быть направлены против целей в реальном мире, где ресурсы ограничены и требуют больших затрат (Nye, 2011, p. 19). В это же время, согласно теории войн четвертого поколения (*fourth-generation warfare*), необходимо использовать все возможные «сети» для того, чтобы убедить лиц, принимающих политические решения со стороны противника, в том, что их политические цели недостижимы или требуют неоправданно больших затрат, что позволяет комбинировать физические и виртуальные атаки для достижения своих целей (Betz & Stevens, 2011, pp. 99–124).

Если еще в далеком прошлом люди просто осознавали значение информации (Jayan, 2009, p. 1) и возможности ее передачи, даже пусть ограниченными средствами, то сегодня бурное развитие ИКТ оказало глубокое влияние на все сферы жизни. Исследуя роль ИКТ в развитии современных видов вооружений в стратегии ведения войн государствами, Т.В. Смит разделяет страны на высокотехнологичные (*hi-tech states*) и невысокотехнологичные (*low-tech countries*) (Smith, 2002). Также справедливо иерархичное разделение стран по их способности оказывать влияние в информационной сфере на тех, кто определяет правила (*rule-maker*), и тех, кто эти правила принимает ввиду отсутствия должного технологического потенциала (*rule-taker*) (Рамич, Пискунов, 2022).

Более того, отдельного внимания заслуживают объекты, используемые для информационно-психологических операций, задача которых — оказать наибольшее влияние на общество и лиц, принимающих решения, через информационные ресурсы. С одной стороны, борьба с дезинформацией и фейками возможна в информационном пространстве с помощью блокировок и инструментов фильтрации контента, а с другой — из-за большого размера информационного пространства физическое уничтожение источника угрозы в сети может быть менее затратным и более эффективным решением проблемы. Так, по данным российских СМИ, 24 февраля 2022 г. одним из первых пораженных объектов на территории Украины был штаб 72-го Центра информационно-психологических операций Вооруженных сил Украины[8]. Это подтверждает значимость информационно-психологических операций в контексте современных конфликтов, но вместе с тем актуализирует вопрос классификации используемых для информационно-психологических операций объектов с точки зрения международного права, особенно в контексте возможного размещения таких объектов не на территории стран — участниц конфликта и возможности привлечения частных подрядчиков.

Таким образом, в рамках данного исследования особое внимание уделяется применению информационно-коммуникационных технологий как средства ведения войны и его совместимости с понятием «гражданского объекта» в современных вооруженных конфликтах.

Применение спутниковых данных сторонами вооруженного конфликта, в частности Украиной, посредством спутниковых станций гражданского назначения (*Starlink*) и других спутниковых данных, предоставляемых третьими странами (странами — членами Организации Североатлантического договора (НАТО) и главным образом США), ставит вопрос о разграничении понятий гражданской и военной ИКТ-инфраструктуры.

Как уже отмечалось, действующие международные инструменты в области международного гуманитарного права не дают полного определения того, что представляет собой «гражданский объект»[9]. Обычно

[8] Альшаева И. «Чтобы не промывали мозги»: ликвидирован штаб «фабрики троллей» ВСУ // Газета.ru. 25.02.2022. URL: https://www.gazeta.ru/army/2022/02/25/14577799.shtml?ysclid=m7ke4nv4ij91060383 (дата обращения: 24.06.2023).

[9] См.: Международное право : в 2 томах. Т. 2: Особенная часть : учебник для вузов. 2-е изд., перераб. и доп. / под ред. А. Я. Капустина. Москва : Изд-во Юрайт, 2025. С. 102; Сассоли М. Законные цели нападения в международном гуманитарном праве // Международный Комитет Красного Креста.

гражданский объект представляется нечто иным, чем «военный объект». Ст. 52 Дополнительного протокола I к Женевским конвенциям 1949 г., касающаяся защиты жертв международных вооруженных конфликтов (далее — Протокол I), определяет, что «*гражданскими объектами являются все те объекты, которые не являются военными объектами*»[10]. В свою очередь второй пункт той же статьи определяет военный объект следующим образом: «*Военные объекты ограничиваются теми объектами, которые в силу своего характера, расположения, назначения или использования вносят эффективный вклад в военные действия и полное или частичное разрушение, захват или нейтрализация которых при существующих в данный момент обстоятельствах дает явное военное преимущество*»[11]. Можно заметить, что само определение «военного объекта» не конкретно, поскольку фраза «Военный объект в силу своего характера… дает явное военное преимущество» в современном контексте требует серьезного уточнения.

Таким образом, формулировка п. 2 ст. 52 Протокола I, как отмечает М. Сассоли, является абстрактной[12] и дает возможность для широкого толкования различными сторонами. В связи с этим неслучайно Т.В. Смит, анализируя действующие нормы МГП, отмечает, что МГП способствует развитию вооружений (Smith, 2002, p. 362).

Однако, исходя из приведенного определения, можно отметить некоторые характеристики военного объекта, касающиеся его характера, расположения и назначения. Данные характеристики должны давать очевидное военное преимущество как обороняющейся стране, так и противнику при его поражении. Как видно, определения «гражданский объект» и «военный объект» из Протокола I способствуют их широкой интерпретации, в том числе среди ученых и специалистов.

В этой связи некоторые авторы пытаются дать свое определение, которое могло бы послужить примером в будущем при разработке и принятии новых международных правовых норм в области МГП или при внесении изменений в действующие инструменты. Например, по мнению Ю.В. Пузыревой, *военными объектами могут являться как объекты, специально созданные для использования в военных целях (боевая техника, заводы по изготовлению боеприпасов, склады военного снаряжения и т. п.), так и гражданские объекты (жилой дом или мост становятся военными объектами в силу их тактического использования обороняющейся стороной)* (Пузырева, 2006).

Как нам представляется, замечание Ю.В. Пузыревой о том, что *не существует объектов, которые были бы исключительно гражданскими или военными,* справедливо, поскольку гражданские объекты, такие как жилые дома, мосты, железнодорожные пути, спутниковые станции, станции электроснабжения и др., в силу их тактического использования обороняющейся стороной могут стать военными объектами и, соответственно, военными законными целями, подтверждение чему можно увидеть в настоящее время на Украине. Например, неправительственная организация *Amnesty International* 4 августа 2022 г. в своем заявлении отметила, что Украина размещает военную технику в населенных пунктах, школах и больницах[13]. В таком случае указанные гражданские объекты становятся законными целями.

23.01.2004. URL: https://web.archive.org/web/20221011205642/https://www.icrc.org/ru/doc/resources/documents/misc/ihl-attacks-230104.htm (дата обращения: 15.05.2023).

[10] Дополнительный Протокол I к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов от 8 июня 1977 года // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/901755843 (дата обращения: 15.05.2023).

[11] Там же.

[12] Сассоли М. Законные цели нападения в международном гуманитарном праве // Международный Комитет Красного Креста. 23.01.2004. URL: https://web.archive.org/web/20221011205642/https://www.icrc.org/ru/doc/resources/documents/misc/ihl-attacks-230104.htm (дата обращения: 15.05.2023).

[13] Ukraine: Military Endangering Civilians by Locating Forces in Residential Areas — New Research // Amnesty International. August 4, 2022. URL: https://www.amnesty.org.uk/press-releases/ukraine-military-endangering-civilians-locating-forces-residential-areas-new (accessed: 15.05.2023).

Следует отметить, что МГП устанавливает одинаковые правила, права и обязанности для сторон конфликта, не разграничивая наступательные и оборонительные операции. Напомним, что во время операции «Буря в пустыне» в 1990–1991 гг. в Ираке из утвержденного странами коалиции списка целей для бомбардировок, включающего 12 объектов, более половины были объектами гражданского назначения: системами электроснабжения, телекоммуникационными системами, мостами, водохранилищами и т. п. (Smith, 2002, p. 364). Подобная тактика уничтожения объектов гражданской инфраструктуры и объектов двойного назначения была также применена в Югославии странами — членами НАТО (Boothby, 2018, p. 7).

Таким образом, четкое определение гражданского объекта особенно актуально в условиях глобализации и скачка развития ИКТ. Все, что ранее использовалось в области информационных технологий только в военных целях, сейчас стало общественным, то есть гражданским достоянием. Все это осложняет определение правового статуса ИКТ в военное время.

У. Бутби справедливо отмечает, что создание радиолокационных систем (*radar*) во время Второй мировой войны и их применение в гражданской авиации способствовало обеспечению безопасности в этой области (Boothby, 2018, p. 7). Это также подтверждает двойное назначение военных объектов в гражданских целях и наоборот. Схожая ситуация наблюдается и в случае со спутниковыми навигационными системами. Изначально американская система глобального позиционирования (*Global Positional* System, GPS) и российская Глобальная навигационная спутниковая система (ГЛОНАСС) носили исключительно военный характер применения. Например, уже в Иракской кампании 1990–1991 гг. Пентагон применял технологии GPS в авиаударах, для того чтобы сделать их более точечными (Smith, 2002, p. 366), а также при управлении высокоточными ракетами. Однако если в то время подобные спутниковые навигационные системы использовались в военных целях, то на современном этапе они получили широкое применение уже в гражданских целях. При этом их первоначальное предназначение не исчерпало себя, и они не только вносят неоценимый вклад в развитие ИКТ гражданского назначения, но и предоставляют существенное военное преимущество при ведении войны сторонами, поскольку они не только определяют геопозицию противника в режиме реального времени, но и могут быть использованы для управления летательными аппаратами.

Дилемма инфраструктуры ИКТ гражданского назначения во время вооруженных конфликтов

Расположение инфраструктуры ИКТ и их двойное назначение ставит ряд вопросов при определении гражданского объекта: например, можно ли поражать *комплекс инфраструктуры информационно-коммуникационных технологий* гражданского назначения, размещенный в жилых домах или в жилых кварталах, если обороняющаяся сторона не переместила их из этих мест и одновременно использует их в военных целях, получая при этом явное военное преимущество. Речь идет, как правило, о спутниковых антеннах и иных средствах вещания, а также иных объектах инфраструктуры, обеспечивающих функционирование средств вещания, таких как объекты электроснабжения, и иных станциях. По действующим Женевским конвенциям эти объекты инфраструктуры среди других гражданских объектов будут защищены только в случае, если есть сомнение в их использовании обороняющейся стороной в военных целях. Однако несмотря на их расположение среди объектов гражданского назначения, они могут стать военными целями в соответствии с Протоколом I, как это происходило во время военных операций в Ираке и Югославии[14].

Конечно, разработчики Женевских конвенций и относящихся к ним протоколов не

[14] Сассоли М. Законные цели нападения в международном гуманитарном праве // Международный Комитет Красного Креста. 23.01.2004. URL: https://web.archive.org/web/20221011205642/https://www.icrc.org/ru/doc/resources/documents/misc/ihl-attacks-230104.htm (дата обращения: 15.05.2023).

могли это предвидеть, а в настоящее время сложно определить, как будут развиваться ИКТ в ближайшие годы. Это большой вызов для современного международного гуманитарного права, и употребляемый нами термин «*комплексная инфраструктура информационно-коммуникационных технологий»* также имеет большое значение. Под *«комплексной инфраструктурой информационно-коммуникационных технологий»* наряду с другим оборудованием, обслуживающим данную сферу деятельности, следует понимать объекты электроснабжения, антенны, башни (телевизионные, телекоммуникационные), пути сообщения, обеспечивающие доступ к этой инфраструктуре или поддерживающие их бесперебойное функционирование, и т. п. Комплексная инфраструктура ИКТ, как показывает практика, является критической инфраструктурой государства, жизненно необходимой для нормального функционирования экономики и иных сфер деятельности страны (Gallais & Filiol, 2017). Комплексная инфраструктура ИКТ неизбежно становится законной военной целью в соответствии со ст. 52, если будет доказано, что обороняющаяся сторона пользуется ею, тем самым обеспечивая себе военное преимущество.

В целях адаптации к меняющимся условиям в НАТО было разработано Таллиннское руководство по международному праву, применимому к кибероперациям, где сформулированы основные понятия и подходы к новым вызовам и угрозам, появившимся в условиях цифровизации. В документе несколько разделов посвящено теме разграничения гражданских и военных объектов в сфере ИКТ. В частности, в норме 100 указывается, что объекты ИКТ-инфраструктуры могут быть признаны военными объектами, если соответствуют одному из четырех критериев: сущность, расположение, назначение и использование[15].

Во-первых, в Таллиннском руководстве разграничено понятие военной цели в юридическом и операционном смысле. Например, оперативной целью может быть нейтрализация передачи электронных сообщений, сами же сообщения в юридическом смысле не будут легальной военной целью, однако оборудование, используемое для их приема и передачи, будет считаться таковым[16].

Во-вторых, компьютеры и другая ИКТ-инфраструктура определяются в качестве военных объектов на основе критерия «сущности», что имеет значение в контексте военного командования, коммуникаций, разведки, слежения и др. С точки зрения положений Таллиннского руководства «военные информационные системы, где бы они ни находились, и объекты, в которых они постоянно располагаются, квалифицируются как военные объекты. Тот факт, что гражданские лица (государственные служащие или подрядчики) могут эксплуатировать эти системы, не имеет отношения к вопросу о том, квалифицируются ли они как военные объекты»[17].

В-третьих, когда гражданские объекты используются в военных целях, они переквалифицируются в военные объекты. Так, «если сторона конфликта использует определенную гражданскую компьютерную сеть в военных целях, эта сеть теряет свой гражданский характер и становится военным объектом, даже если она продолжает использоваться в гражданских целях»[18]. Также военным объектом будет считаться предприятие, производящее компьютерное оборудование по контракту с вооруженными силами противника, даже если на этом же предприятии производятся товары гражданского назначения[19].

В-четвертых, объект может быть признан военным по критериям «расположения», которое может дать одной из сторон военное преимущество, или по «назначению», которое позволяет использовать объект в военных целях в будущем[20].

Существует несколько примеров, когда гражданские объекты были переквалифицированы в военные из-за соответствия указанным критериям.

[15] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by M. N. Schmitt. Cambridge : Cambridge University Press, 2017. P. 435–445.

[16] Ibid. P. 436.
[17] Ibid. P. 438.
[18] Ibid. P. 438–439.
[19] Ibid.
[20] Ibid. P. 439–440.

Первый пример имеет отношение к операции «Союзная сила» 1999 г. Тогда НАТО объясняла бомбардировку телецентра в Белграде военной необходимостью, утверждая, что телевидение являлось инструментом пропаганды властей страны[21] и, соответственно, обоснованно является военной целью.

Второй пример связан с конфликтом на Украине. В Российской Федерации 8 октября 2022 г. на Крымском мосту произошел взрыв, который привел к частичному обрушению объекта. Результаты расследования, проведенного российскими спецслужбами, подтвердили украинский след в данном инциденте[22], хотя официально руководство страны в лице президента Украины В.А. Зеленского отрицало причастность Киева к данному взрыву[23]. Комментируя случившееся в программах западных (в частности французских) телеканалов, многие эксперты рассматривали Крымский мост в качестве законной военной цели для Украины, то есть он был приравнен к военным объектам, так как предоставлял России военное преимущество[24], несмотря на то, что сам мост является единственной связующей артерией между российской частью материка и полуостровом. Западные эксперты ссылаются на то, что российские войска пользуются данным маршрутом для снабжения военных подразделений при проведении Специальной военной операции (СВО)[25].

Следует отметить, что взрыв на Крымском мосту изменил ход СВО, поскольку после него российская армия начала атаковать важные объекты энергетической инфраструктуры Украины, хотя до этого инцидента удары, по словам российского военного руководства, наносились исключительно по военной инфраструктуре[26]. При этом удары по объектам стратегической инфраструктуры Украины, согласно ст. 52 Протокола I, также являются военной необходимостью, то есть юридически обоснованными целями, поскольку *этой же комплексной инфраструктурой* Украина пользуется для нанесения ударов по российским войскам и по территории Российской Федерации.

В этот же ряд можно поставить передачу Соединенными Штатами Украине станций спутниковой связи *Starlink*, что обеспечивает последнюю военным преимуществом, поскольку эта система используется не только для связи, но и для управления беспилотными летательными аппаратами (БПЛА)[27] для сбора данных и т. п. в ходе военных действий. Соответственно украинская *комплексная стратегическая ИКТ-инфраструктура* становится очевидной законной целью для российских войск: система электроснабжения, спутниковые антенны, железнодорожные пути и др., образующие и обеспечивающие комплексность ИКТ-инфраструктуры Украины, вносят большой вклад «в возможности неприятеля сражаться или поддерживать военные усилия», как пишет Д.С. Маликов (Маликов, 2014, с. 166). Автор также справедливо отмечает, что определенные страны при выборе цели «будут учитывать военное преимущество, ожидаемое от нападения в це-

[21] Сассоли М. Законные цели нападения в международном гуманитарном праве // Международный Комитет Красного Креста. 23.01.2004. URL: https://web.archive.org/web/20221011205642/https://www.icrc.org/ru/doc/resources/documents/misc/ihl-attacks-230104.htm (дата обращения: 15.05.2023). См. также: (Smith, 2002, p. 366).

[22] ФСБ опубликовала материалы о том, как готовился взрыв на Крымском мосту // РИА Новости. 12.10.2022. URL: https://ria.ru/20221012/most-1823287523.html?ysclid=m7kenlrrnq537442668 (дата обращения: 15.05.2023).

[23] Полякова В. Зеленский заявил, что Киев не заказывал теракт на Крымском мосту // РБК. 20.10.2022. URL: https://www.rbc.ru/politics/20/10/2022/63513b7b9a7947798da528f5?ysclid=m7keovvc4k585403941 (дата обращения: 15.05.2023).

[24] Sauvage G. L'attaque du pont de Crimée, point culminant des revers russes en Ukraine // France24. 12.10.2022. URL: https://www.france24.com/fr/europe/20221009-guerre-en-ukraine-le-pont-de-crim%C3%A9e-touch%C3%A9-la-russie-accumule-les-revers (accessed: 19.01.2023).

[25] Ibid.

[26] Брифинги // Министерство обороны Российской Федерации. URL: https://z.mil.ru/spec_mil_oper/brief/briefings.htm (дата обращения: 01.11.2024).

[27] Илон Маск отказался бесплатно поставлять Украине спутниковый интернет // CNews. 14.10.2022. URL: https://www.cnews.ru/news/top/2022-10-14_ilon_mask_otkazalsya_besplatno (дата обращения: 29.11.2022).

лом, а не от отдельных его частей» (Маликов, 2014, с. 166). Кроме того, согласно п. 2 ст. 52, важное место среди признаков военного объекта занимает его расположение.

Однако с учетом комплексности ИКТ-инфраструктуры в данном случае можно заметить, что даже обычные спутниковые антенны, расположенные на частных домах в населенных пунктах, в современных реалиях становятся военными законными целями при ведении войны, поскольку они обеспечивают военное преимущество противника, о чем свидетельствуют действия НАТО в Ираке и Югославии.

Следовательно, возникает вопрос, как восполнить пробел в нормах международного гуманитарного права с учетом современных реалий развития ИКТ, поскольку, с нашей точки зрения, этот процесс будет только усугублять ситуацию, связанную с проблемой разграничения гражданского и военного объектов, как показывает анализ некоторых современных средств и методов ведения войны. Классические способы ведения войны, на которых были основаны нормы Женевских конвенций и Протоколов к ним, уже устарели[28]. Сегодня ключевую роль в тактике ведения войны играют не только обычные виды вооружения (например, артиллерия), но и БПЛА и др., использующие ИКТ для передачи данных. В этих условиях обычный инженер, работающий в частной компании и собирающий датчики, беспилотные летательные аппараты, или даже простой IT-специалист может обеспечивать существенное преимущество в ходе конфликта, что не было предусмотрено ранее разработчиками различных норм международного гуманитарного права.

М. Сассоли, обращаясь к комментариям к немецкому военному Уставу, касательно нападения на гражданское население справедливо отмечает следующее: «Если бы намерение оказать непосредственное влияние на решимость народа неприятельской стороны сражаться было признано законной целью применения военной силы, в войне не осталось бы никаких ограничений»[29]. Также с учетом того, что конечная цель международного гуманитарного права, по оговорке Ф.Ф. Мартенса (Кукушкина, Иойрыш, Шишкин, 2019, с. 160), направлена на смягчение и минимизацию последствий военных действий на гражданское население конфликтующих сторон, считаем, что необходимо изъять из военных целей, перечисленных в ст. 52 Дополнительного протокола I, гражданские объекты, в том числе объекты ИКТ-инфраструктуры, даже если они носят двойной характер, особенно при их расположении в населенных пунктах, поскольку экспертные комментарии к статьям Женевских конвенций не содержат перечня обязательств стран-участниц по отношению к таким объектам.

В этой связи следует ужесточить ответственность воюющих сторон за нападение на объекты ИКТ-инфраструктуры или гражданские объекты двойного назначения, а также за их использование в военных целях, если эти объекты преимущественно применяются в гражданских целях как часть ИКТ-инфраструктуры. Подобный подход уже существует в МГП: речь идет о запрете наносить удары по ядерным или иным опасным источникам (например, ГЭС, АЭС, дамбам), несмотря на их назначение (военное или гражданское) и расположение, то есть близости/дальности к населенным пунктам (Boothby, 2018, p. 52). Это позволяет сохранить жизни мирных людей во время войны. Считаем, что аналогичная трактовка может также быть применена к ИКТ-инфраструктуре.

Также следовало бы, как отметил М. Сассоли, вести список, четко определяющий гражданские объекты, используемые как военные, с возможностью внесения изменений с учетом развития современных ИКТ или международных отношений в целом.

Отдельным важным аспектом является возможность использования ИКТ для нанесения ущерба государству без фактического

[28] Сассоли М. Законные цели нападения в международном гуманитарном праве // Международный Комитет Красного Креста. 23.01.2004. URL: https://web.archive.org/web/20221011205642/https://www.icrc.org/ru/doc/resources/documents/misc/ihl-attacks-230104.htm (дата обращения: 15.05.2023).

[29] Там же.

начала боевых действий. Это может быть кибератака на критическую инфраструктуру или значимые для социальной или государственной жизни объекты. Основной проблемой является определение «порога», который можно считать допустимым для того, чтобы считать кибератаку нарушением суверенитета со всеми вытекающими последствиями в рамках международного гуманитарного права.

Возможным решением в рамках текущего этапа разработки международных правил в сфере ИКТ может быть «мягкое регулирование», позволяющее предварительно определить нормы и правила поведения посредством участия многосторонних организаций и в дальнейшем заложить эти нормы в проекты международно-правовых документов ООН. Подобная ситуация сложилась вокруг принятия международной конвенции в сфере информационной безопасности, где присутствует два подхода: российский подход, предусматривающий уважение нерушимости суверенитета в ходе борьбы с преступным использованием ИКТ, и западный подход, подразумевающий «возможность борьбы с киберпреступностью без учета государственного суверенитета», что «фактически предполагает экстерриториальное распространение права сильного в данной области»[30]. Соответственно нормы, предлагаемые Россией, также легли в основу концепции Конвенции ООН об обеспечении международной информационной безопасности и документов, принятых в Шанхайской организации сотрудничества (ШОС) и БРИКС, а нормы, предлагаемые западными странами, поддерживаются США и приняты в НАТО и Европейском союзе.

[30] Зиновьева Е. С. Международная информационная безопасность в двусторонних отношениях России и США // Российский совет по международным делам. 22.02.2023. URL: https://russiancouncil.ru/analytics-and-comments/analytics/mezhdunarodnaya-informatsionnaya-bezopasnost-v-dvustoronnikh-otnosheniyakh-rossii-i-ssha/?sphrase_id=101081028 (дата обращения: 26.06.2023).

Заключение

Подводя итоги исследования, можно отметить, что проблема разграничения гражданских и военных объектов весьма актуальна. Данное разграничение становится с каждым днем все более размытым, особенно в условиях развития современных информационно-телекоммуникационных технологий. Проведенный нами анализ продемонстрировал, что западные страны, в частности государства — члены НАТО, в своей практике считают гражданские объекты двойного назначения военными объектами, как было показано при проведении военных кампаний в Ираке, сербском Косово и др. Таким образом, ИКТ, безусловно, открывают большие возможности в различных областях человеческой жизни. Однако по большому счету их первоначальное назначение в области военной сферы по-прежнему остается первостепенным, несмотря на их широкое введение в гражданский оборот, что будет в дальнейшем осложнять не только разграничение понятия гражданских и военных объектов, но и установление ответственности воюющих сторон за нарушение МГП.

Большинство объектов ИКТ-инфраструктуры являются объектами двойного назначения, что создает сложность в их классификации в качестве гражданских или военных целей. Помимо этого, возможность удаленного доступа и нанесения кибератак из «третьих стран» ставит вопрос законных мер противодействия и «порога» нанесенного ущерба для реализации тех или иных ответных мер.

Сложность в принятии новых международных норм и правил также связана с различными подходами стран к пониманию киберпространства и суверенитета в киберпространстве, что становится причиной кластеризации государств, придерживающихся тех или иных взглядов, и формирования нормативных документов на базе региональных международных организаций.

Поступила в редакцию / Received: 18.10.2023
Доработана после рецензирования / Revised: 04.11.2024
Принята к публикации / Accepted: 24.12.2024

Библиографический список

Блищенко И. П. Обычное оружие и международное право. Москва : Международные отношения, 1984.

Кукушкина А. В, Иойрыш А. И., Шишкин В. Н. Международное гуманитарное право и оговорка Мартенса // Закон и право. 2019. № 9. С. 159–163. https://doi.org/10.24411/2073-3313-2019-10431; EDN: URLACB

Маликов Д. С. К вопросу об определении понятий военных и гражданских объектов в районах вооруженного конфликта и о правовой оценке различий между ними // Власть. 2014. № 8. С. 163–168. EDN: SJXJHX

Пузырева Ю. В. Разграничение гражданских и военных объектов в международном гуманитарном праве // Юрист-международник. 2006. № 4. С. 19–28. EDN: UWCVMH

Рамич М. С., Пискунов Д. А. Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 238–255. https://doi.org/10.22363/2313-0660-2022-22-2-238-255; EDN: KSSXFK

Фуркало В. В. Международно-правовая защита гражданского населения в период вооруженных конфликтов: дис. … канд. юр. наук. Киев, 1982. EDN: NPLCHL

Betz D. J., Stevens T. Cyberspace and the State: Toward a Strategy for Cyber-Power. Abingdon : Routledge, 2011. URL: https://www.researchgate.net/publication/345705816_Cyberspace_and_the_State_Toward_a_Strategy_for_Cyber-power (accessed: 12.10.2024).

Boothby W. H. New Technologies and the Law in War and Peace. Cambridge : Cambridge University Press, 2018. https://doi.org/10.1017/9781108609388

Dinstein Y. The Principle of Distinction and Cyber War in International Armed Conflicts // Journal of Conflict and Security Law. 2012. Vol. 17, iss. 2. P. 261–277. https://doi.org/10.1093/jcsl/krs015

Gallais C., Filiol E. Critical Infrastructure: Where Do We Stand Today? A Comprehensive and Comparative Study of the Definitions of a Critical Infrastructure // Journal of Information Warfare. 2017. Vol. 16, iss. 1. P. 64–87. URL: https://www.jstor.org/stable/26502877 (accessed: 16.06.2024).

Jayan S. D. About Information, Information Technology, Cryptography and Law // Journal of the Indian Law Institute. 2009. Vol. 51. P. 1–11. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1804899# (accessed: 26.06.2024).

Nye J. S. Nuclear Lessons for Cyber Security? // Strategic Studies Quarterly. 2011. Vol. 5, no. 4. P. 18–38. URL: https://www.jstor.org/stable/26270536 (accessed: 26.06.2024).

Routledge Handbook of the Law of Armed Conflict / ed. by R. Liivoja, T. McCormack. London : Routledge, 2016. https://doi.org/10.4324/9780203798362

Schmitt M. N. The Principle of Distinction and Weapon Systems on the Contemporary Battlefield // Connections. 2008. Vol. 7, no. 1. P. 46–56. https://doi.org/10.11610/Connections.07.1.03

Smith T. W. The New Law of War: Legitimizing Hi-Tech and Infrastructural Violence // International Studies Quarterly. 2002. Vol. 46, no. 3. P. 355–374. https://doi.org/10.1111/1468-2478.00237

Сведения об авторах:

Аду Яо Никэз — кандидат юридических наук, доцент кафедры теории и истории международных отношений, Российский университет дружбы народов; доцент кафедры теории государства и права и конституционного права, Оренбургский государственный университет; почетный профессор, Уральский государственный экономический университет; eLibrary SPIN-код: 6740-9517; ORCID: 0000-0001-8696-0181; e-mail: adu-ya@rudn.ru

Рамич Мирзет Сафетович — ассистент кафедры теории и истории международных отношений, Российский университет дружбы народов; научный сотрудник Центра прикладного анализа международных трансформаций, Российский университет дружбы народов; eLibrary SPIN-код: 1830-1087; ORCID: 0000-0003-1479-2785; e-mail: ramich_ms@pfur.ru