Кибератаки на установки, содержащие опасные силы: телеологическое основание применимости режима статьи 56 дополнительного протокола I

Климов Ярослав Игоревич
ассистент кафедры гуманитарных наук, Финансовый университет при Правительстве Российской Федерации; соискатель кафедры международного и интеграционного права, юридический факультет, Института права и национальной безопасности им. М. М. Сперанского, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, kyai@mail.ru

Статья посвящена нормативному обоснованию применимости специального запрета нападений на установки, содержащие опасные силы (статья 56 Дополнительного протокола I к Женевским конвенциям 1977 г., ДП I), к кибератакам на системы управления охраняемых объектов. Посредством телеологического толкования нормы по правилу статьи 31(1) Венской конвенции о праве международных договоров 1969 г. установлено: запрет статьи 56(1) ДП I ориентирован на последствие (высвобождение опасных сил), а не на инструмент воздействия, и потому охватывает кибератаки без создания нового договорного инструмента. Функциональный подход МККК (доклад 32IC/15/11, 2015 г.) и Правило 82 Таллиннского руководства 2.0 подтверждают этот вывод. Сравнительный анализ позиций шести государств выявил структурную асимметрию: государства с наибольшим кибернаступательным потенциалом располагают наименее определёнными договорными обязательствами по статье 56 ДП I. Выделены три структурных пробела режима: текстуальный (разрешимый телеологическим толкованием делеге-лата), операциональный (требующий вторичных инструментов) и атрибуционный (не устранимый средствами толкования). Де-леге-ферента предложены три взаимодополняющие меры с оценкой их политической реализуемости.

Ключевые слова: международное гуманитарное право, кибератаки, телеологическое толкование, установки с опасными силами, Таллиннское руководство 2.0, атрибуция, *de lege ferenda*, МККК, *opinio juris*, Stuxnet.

Введение

В сентябре 2015 г. МККК квалифицировал кибератаки против ядерных электростанций и гидрологических объектов как «колоссальную угрозу» и подтвердил применимость ограничений международного гуманитарного права к таким операциям [1]. Пятью годами позднее Генеральный секретарь ООН зафиксировал нарастание угрозы кибератак против объектов электро- и водоснабжения в условиях вооружённых конфликтов [2]. Оба документа указывают на один нерешённый правовой вопрос: охватывает ли специальный режим статьи 56 ДП I атаки против охраняемых установок, осуществлённые посредством кибероружия, если они способны произвести тот же результат, что и прямой кинетический удар?

Норма принималась в 1977 г., когда цифровые промышленные системы управления (SCADA, ICS, DCS) не существовали как технологический класс; программируемые логические контроллеры появились в атомной энергетике лишь в 1980-х гг. Статья 56(1) ДП I запрещает «нападения» на дамбы, плотины и атомные электростанции, не конкретизируя метод воздействия [4]. При ограничительном прочтении «нападения» как исключительно кинетического удара кибератака на систему управления реактором выводится за пределы специального режима и оказывается под действием общего запрета по статье 52(2) ДП I, где порог квалификации объекта в качестве военной цели существенно ниже. Именно эта правовая неопределённость составляет предмет настоящего исследования.

Статья исходит из тезиса, что правильным методом разрешения указанной неопределённости является телеологическое толкование по правилу статьи 31(1) Венской конвенции о праве международных договоров 1969 г. [5] Аналогия в строгом юридическом смысле предполагает пробел в праве, восполняемый по сходству с близкородственной нормой. Телеологическое толкование пробела не признаёт: запрет статьи 56(1) ориентирован на последствие, а не на инструмент, и потому уже охватывает кибератаки. Разграничение принципиально: оно определяет, требует ли применение нормы нового договорного инструмента или действующего обязательства достаточно.

Научная новизна статьи складывается из трёх позиций. Впервые в отечественной доктрине проведён совокупный анализ договорного обязательства Российской Федерации по статье 56 ДП I, функционального подхода МККК и Правила 82 Таллиннского руководства 2.0 применительно к кибератакам, с методологическим разграничением телеологического толкования и аналогии. Сравнительный анализ шести государственных позиций выявил асимметрию, остававшуюся практически без внимания в доктрине. Атрибуционный пробел квалифицирован как самостоятельная правовая проблема, принципиально отличная от вопроса о применимости нормы.

1. Конструкция нормы: запрет через последствие

Статья 56(1) ДП I запрещает нападения на дамбы, плотины и атомные электростанции, если они «могут вызвать высвобождение опасных сил» и причинить «тяжёлые потери» среди гражданского населения [4]. Перечень охраняемых объектов исчерпывающий. Специальная защита снимается лишь при одновременном выполнении тройного критерия статьи 56(2): регулярная, существенная и непосредственная военная поддержка, оказываемая объектом противнику, при условии невозможности достичь того же результата иными средствами. В. А. Батырь констатирует, что отсутствие хотя бы одного из трёх элементов сохраняет специальный иммунитет в полном объёме [7, с. 50]. Комментарий МККК 1987 г. уточняет: обеспечение армии электроэнергией от атомной электростанции само по

себе «непосредственной» поддержки в смысле тройного критерия не образует [6].

Понятие «нападения» по статье 49(1) ДП I охватывает «акты насилия против противника» без ограничения способом осуществления [4]. Запрет строится через последствие, а не через описание применяемого оружия. Руководство HPCR 2013 г. воспроизводит ту же логику в Правиле 36: особая осторожность при нападениях на охраняемые объекты требуется вне зависимости от применяемого вооружения или метода воздействия [9]. Кибератака на SCADA-систему реактора, влекущая разрушение системы охлаждения или неконтролируемый выброс радиоактивных материалов, соответствует условиям запрета статьи 56(1) ДП I.

G. Biggio обосновал в 2025 г. применение концепции «Loss of Functionality» к принципам различения и соразмерности ДП I: некинетические последствия кибератак учитываются при оценке сопутствующего ущерба по тем же стандартам, что и физические повреждения [10, с. 251–255]. Для объектов статьи 56 этот вывод особенно весом: авария на ядерном объекте или прорыв плотины по последствиям необратимы, и расчёт соразмерности применительно к ним структурно не работает. Именно поэтому статья 56 конструирует иммунитет как абсолютный.

Вопрос о методологических пределах телеологического толкования требует специального рассмотрения. Й. Динштейн настаивает на строгом конструктивизме при расширении понятия «нападение» за пределы кинетического насилия: в его прочтении статья 49(1) ДП I содержит имплицитное указание на физическое принуждение, а нефизическое воздействие требует прямого указания в тексте нормы [13, с. 209–212]. Позиция корректна для большинства норм МГП, где буквальное толкование устойчиво. Применительно к статье 56 она порождает практический парадокс: если кибератака на систему охлаждения реактора с технической вероятностью влечёт именно то последствие, против которого норма направлена, строгое конструктивистское прочтение фактически выводит её из-под нормы по формальному признаку. Комментарий МККК 1987 г. прямо указывает, что смысл нормы состоит в предотвращении «катастрофических и необратимых последствий» для гражданского населения [6]. Кибератака, влекущая именно такие последствия, охватывается нормой по функции.

2. Позиция МККК и функциональный подход

В докладе 32IC/15/11 (2015 г.) МККК указал, что ограничения МГП применяются к кибератакам против ядерных объектов и дамб «по аналогии» [1]. Как разграничено выше, в данном контексте термин «аналогия» обозначает телеологическое распространение той же *ratio legis* на новую форму воздействия, а не восполнение пробела. Функциональный подход исходит из того, что норма охватывает любой акт, способный произвести запрещённый результат.

Руководящие принципы МККК 2020 г. по охране природной среды в вооружённых конфликтах закрепили двойной стандарт в Правиле 11 [11]. Государства – участники ДП I связаны договорным запретом нападений, способных высвободить опасные силы (Правило 11.B); для остальных государств действует обычно-правовое требование особой осторожности по Правилу 42 Исследования МККК 2005 г. [8, с. 141]. Оба стандарта строятся через последствие. Документ МККК 2025 г. о вовлечённости гражданских лиц в кибероперации подтверждает последовательность этой позиции: принципы МГП применяются к кибератакам системно [12].

3. Таллиннское руководство 2.0: Правило 82 и opinio juris

Таллиннское руководство 2.0, изданное под редакцией М. Шмитта, содержит наиболее систематизированный доктринальный свод по применению международного права к кибероперациям. Правило 82 устанавливает прямой запрет: кибератаки против плотин, дамб и атомных электростанций недопустимы, если они «ожидаемо высвободят опасные силы» [3, с. 469]. Структура Правила воспроизводит статью 56(1) ДП I, заменяя «нападение» на «кибератаку».

Среди разработчиков Руководства были специалисты из государств с наибольшим кибернаступательным потенциалом: США, Великобритании, Германии, Франции и Нидерландов. Ни один из них не предложил правового обоснования допустимости кибератак на объекты статьи 56. Для оценки *opinio juris* по критерию статьи 38(1)(b) Статута Международного суда ООН это существенно: отсутствие публичных возражений при очевидной осведомлённости о проблеме образует релевантный элемент *opinio juris*. О. Помсон в 2023 г. показал: при установлении применимости норм обычного международного права к кибероперациям необходимо выявлять, распространялось ли *opinio juris* государств именно на данную форму поведения [14, с. 1034]. Группа правительственных экспертов ООН в докладе A/76/135 (2021 г.) подтвердила консенсусом государств, что МГП применяется к кибероперациям в период вооружённого конфликта [15, с. 10].

4. Государственные позиции: структурная асимметрия

Сравнение государственных позиций выявляет закономерность, практически не отмеченную в доктрине. Государства с наибольшим кибернаступательным потенциалом располагают наименее определёнными правовыми ограничениями по статье 56 ДП I; государства с наиболее прочным договорным основанием запрета декларируют сдержанность в сфере наступательных кибероопераций. Ни одно из шести рассмотренных государств публично не заявило о правомерности кибератак на дамбы, плотины и атомные электростанции.

Российская Федерация ратифицировала ДП I 29 сентября 1989 г. без оговорок к статье 56. Наставление по МГП для Вооружённых Сил Российской Федерации 2001 г. обязывает военнослужащих на этапе планирования операций наносить на карты атомные электростанции, дамбы и плотины. В. А. Батырь оценивает это требование как действующее вне зависимости от дискуссий об обычно-правовом статусе соответствующих положений [23, с. 18]. А. В. Кудашкин и Н. Н. Мельник характеризуют принцип соразмерности как «центральный регулятор при принятии решений» о применении военной силы [24, с. 4]; для объектов статьи 56 этот принцип структурно исключает любой положительный расчёт, поскольку последствия аварии на ядерном объекте несоразмерны любому достижимому тактическому преимуществу.

США к ДП I не присоединились. Сборник Военно-морского колледжа 2012 г. прямо фиксирует, что претензии на обычно-правовой статус положений Дополнительных протоколов «вызывают обеспокоенность» американской стороны [26, с. 9–10]. Американская правовая доктрина по кибератакам развивалась преимущественно через призму *jus ad bellum* (статья 51 Устава ООН), а не специальных режимов *jus in bello*. Государство с наибольшим кибернаступательным потенциалом в мире максимально сохраняет правовую свободу действий применительно к объектам, нападение на которые статья 56 запрещает.

Франция в доктринальном документе 2019 г. прямо распространила принципы различения и соразмерности на кибератаки [16, с. 7–8]; решение об атрибуции квалифицируется там как политическое и принимается в каждом конкретном случае. Великобритания в позиции, представленной в ГПЭ ООН в 2021 г., подтвердила применимость МГП к кибероперациям и констатировала отсутствие нормы, обязывающей публично раскрывать технические основания атрибуции [17, с. 6].

КНР ратифицировала ДП I 14 декабря 1983 г. и формально связана запретом статьи 56. Хуан Чжэньюй и Ин Ин показывают, что китайский подход акцентирует *jus ad bellum*-измерение кибербезопасности при сдержанном позиционировании в части *jus in bello* применительно к конкретным нормам ДП I [18, с. 206–210]. К. К. Лазарь фиксирует, что Россия и КНР, продви-

гая концепцию киберсуверенитета, концентрируются на недопустимости внешнего вмешательства, тогда как детализация специальных режимов МГП в национальных доктринах обеих стран остаётся менее проработанной [19, с. 185]. Израиль в 2020 г. занял «осторожную» позицию по применению МГП к кибероперациям в вооружённом конфликте [20]; публичной позиции по статье 56 применительно к кибератакам от Израиля не поступало.

Выявленная асимметрия имеет самостоятельное доктринальное значение. Эффективность режима статьи 56 ДП I применительно к кибератакам зависит в первую очередь от добровольного соблюдения нормы теми государствами, которые юридически к ней наименее обязаны. Такой разрыв между договорными обязательствами и кибернаступательными возможностями существенно осложняет переговорный процесс о новых договорных инструментах и требует учёта при оценке политической реализуемости предложений *de lege ferenda*.

5. Stuxnet и Industroyer: правовая оценка инцидентов

Два задокументированных инцидента позволяют оценить применимость статьи 56 ДП I к близким к реальным сценариям. Stuxnet (2010) был направлен против центрифуг по обогащению урана в Натанзе. К. Зеттер детально реконструировала технический механизм: код воздействовал на контроллеры Siemens STEP 7 и вызывал механическое разрушение центрифуг при внешне нормальных показаниях мониторинговых систем [21, с. 34–89]. Объект в Натанзе является объектом ядерного цикла, а не атомной электростанцией в смысле статьи 56(1) ДП I. Тем не менее Stuxnet подтвердил три принципиальные вещи: физические разрушения через SCADA-атаки на ядерную инфраструктуру технически реализуемы; кибератака способна производить результаты, физически эквивалентные кинетическому воздействию; атрибуция в реальном времени недостижима.

Если бы атака типа Stuxnet была направлена против систем управления охлаждением реактора на действующей атомной электростанции, правовая квалификация была бы принципиально иной. Манипуляция программным обеспечением охлаждения активной зоны с технической вероятностью влечёт аварийный перегрев и выброс радиоактивных материалов: именно это последствие, которое статья 56(1) характеризует как «высвобождение опасных сил». Запрет применился бы независимо от того, каким является применяемый инструмент.

Industroyer/CrashOverride (2016) поставил под угрозу электроснабжение части Киева, воздействуя на подстанцию Ukrenergo. Объект атаки является электросетью, а не установкой с опасными силами по статье 56. ESET идентифицировала группу Sandworm спустя год; американские обвинительные заключения были предъявлены в 2020 г. В период самой атаки атрибуция оставалась технически недостижимой. М. Рошини обосновал: кибератака, производящая физически эквивалентный кинетическому удару эффект, оценивается по тем же критериям МГП [22, с. 152–157]. Оба инцидента документируют атрибуционный барьер как ключевое практическое ограничение режима ответственности.

6. Три структурных пробела режима

Пробелы режима статьи 56 применительно к кибератакам принципиально различны по природе. Их смешение влечёт предложение неверных решений.

Первый пробел, текстуальный, разрешается *de lege lata* через телеологическое толкование: государства, ратифицировавшие ДП I без оговорок к статье 56, связаны запретом без нового договорного инструмента. Второй пробел операциональный: кибератака на управляющую систему не разрушает объект напрямую, физические последствия развиваются через цепочку отказов. Статья 56(1) оперирует критерием угрозы («способные вызвать»). Комментарий МККК 1987 г. подтверждает, что запрет вступает в действие на стадии создания реального риска [6]; применить этот критерий к каскадному воздействию без операциональной конкретизации действующий текст ДП I не позволяет. Пробел устраним через вторичные инструменты без пересмотра договорного текста.

Третий пробел, атрибуционный, принципиально отличается от первых двух. Он не затрагивает содержание запрета: запрет функционирует *de lege lata*. Он затрагивает режим ответственности. Кибератаки атрибутируются через многоэтапный технический анализ, нередко занимающий годы; результаты систематически оспариваются. Т. Вестнер в 2025 г. указал на смежный риск: алгоритмизация планирования операций, не включающая специальный иммунитет статьи 56 применительно к кибератакам, генерирует неверный правовой результат уже на предоперационном этапе [25, с. 215–219]. Атрибуционный пробел не закрывается средствами толкования.

7. De lege ferenda: три меры

Первое предложение: факультативный протокол к ДП I с метод-нейтральным стандартом. Документ должен закрепить, что запрет нападений на объекты статьи 56(1) распространяется на любой акт, независимо от применяемого инструмента, если он ожидаемо способен вызвать высвобождение опасных сил. МККК обозначил это направление в 2015 г. [1]; Правило 82 Таллиннского руководства показало, что метод-нейтральный стандарт может быть корректно сформулирован [3, с. 469–473]. Политически эта мера нереалистична в краткосрочной перспективе: государства с наибольшим кибернаступательным потенциалом не заинтересованы в жёстких запретительных нормах, прямо упоминающих кибератаки.

Второй вариант: верификационный механизм для кибератак на ядерные и гидрологические объекты под эгидой МАГАТЭ или ООН, активируемый при появлении достоверной информации о кибератаке без предварительного консенсуса по атрибуции. Прецедент существует: Инспекционная и вспомогательная миссия МАГАТЭ действует на Запорожской АЭС с сентября 2022 г. в условиях отсутствия консенсуса об ответственности; её задача состоит в верификации безопасности, а не в атрибуции. Эта мера политически более достижима, поскольку опирается на существующую институциональную практику.

Третья мера реализуема без международного переговорного процесса: закрепление обязательной правовой классификации кибератак против объектов статьи 56 в документах юридической службы вооружённых сил государств – участников ДП I. Соотношение статьи 56 ДП I с Таллиннским руководством 2.0 в российских учебных программах по праву вооружённых конфликтов отсутствует; включение в предоперационные процедуры обязательной правовой оценки кибератак против охраняемых объектов реализуется приказом Министра обороны. Три предложения взаимодополняют: первое формирует договорную основу, второе создаёт институциональный механизм верификации, третье встраивает запрет в операциональную практику вооружённых сил.

Заключение

De lege lata режим статьи 56 ДП I охватывает кибератаки через телеологическое толкование нормы. Запрет статьи 49(1) ДП I не ограничен способом осуществления нападения; статья 56(1) строится через последствие. Государства, ратифицировавшие ДП I без оговорок к статье 56, включая Российскую Федерацию, связаны этим запретом. Позиция МККК (доклад 32IC/15/11, 2015 г.) и Правило 82 Таллиннского руководства 2.0 подтверждают этот вывод; ни одно государство не выдвинуло правового обоснования допустимости кибератак на охраняемые объекты.

Сравнительный анализ выявил структурную асимметрию: государства с наибольшим кибернаступательным потенциалом располагают наименее определёнными договорными обязательствами по статье 56 ДП I. Россия, ратифицировавшая ДП I безоговорочно, располагает наиболее прочным нормативным основанием запрета среди крупных военных держав. Stuxnet и Industroyer документируют техническую реализуемость охватываемых запретом сценариев и подтверждают атрибуционный

барьер как ключевое практическое ограничение режима ответственности.

Три выявленных структурных пробела принципиально различны. Текстуальный разрешён *de lege lata*. Операциональный требует уточнения вторичными инструментами. Атрибуционный является наиболее критическим: запрет функционирует, тогда как режим ответственности нереализуем без специального верификационного механизма. Предложенные три меры *de lege ferenda* адресуют эти пробелы последовательно и независимо друг от друга. Строгий запрет *de lege lata* существует. Проблема состоит в его практическом обеспечении.

В отличие от предшествующих работ, рассматривавших позицию МККК, Таллиннское руководство и российское обязательство по статье 56 раздельно, настоящая статья устанавливает их системную связь применительно к кибератакам и разграничивает три структурных пробела по природе. Новизна состоит также в выявлении асимметрии между договорными обязательствами и кибернаступательными возможностями государств как самостоятельной правовой проблемы, определяющей реальную реализуемость запрета.

Литература

1. International humanitarian law and the challenges of contemporary armed conflicts: Report 32IC/15/11. – Geneva : ICRC, 2015. – 58 p.
2. Защита гражданских лиц в вооружённом конфликте : доклад Генерального секретаря ООН (S/2020/366). – Нью-Йорк : ООН, 2020. – 21 с.
3. Schmitt M. N. (ed.) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. – Cambridge : Cambridge University Press, 2017. – 598 p. DOI: 10.1017/9781316822524.
4. Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооружённых конфликтов (Протокол I). Женева, 08.06.1977 // UN Treaty Series. Vol. 1125. No. 17512.
5. Венская конвенция о праве международных договоров. Вена, 23.05.1969 // UN Treaty Series. Vol. 1155. No. 18232.
6. Sandoz Y., Swinarski C., Zimmermann B. (eds.) Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. – Geneva : ICRC ; Martinus Nijhoff, 1987. – 1625 p.
7. Батырь В. А. Международно-правовая охрана отдельных территориальных объектов в период вооружённых конфликтов // Право в Вооружённых Силах. – 2023. – № 8. – С. 44–55. EDN: YXRUJX.
8. Henckaerts J.-M., Doswald-Beck L. (eds.) Customary International Humanitarian Law. Vol. I : Rules. – Cambridge : Cambridge University Press ; ICRC, 2005. – 621 p. DOI: 10.1017/CBO9780511804700.
9. HPCR Manual on International Law Applicable to Air and Missile Warfare. – Cambridge : Cambridge University Press, 2013. – 441 p. DOI: 10.1017/CBO9781139525275.
10. Biggio G. Regulating non-kinetic effects of cyber operations: the 'Loss of Functionality' approach and the military necessity-humanity balance under International Humanitarian Law // Journal of Conflict and Security Law. – 2025. – Vol. 30, no. 2. – P. 241–263. DOI: 10.1093/jcsl/kraf008.
11. Guidelines on the Protection of the Natural Environment in Armed Conflict. – Geneva : ICRC, 2020. – 128 p.
12. IHL and the Growing Involvement of Civilians in Cyber Operations. – Geneva : ICRC, 2025.
13. Dinstein Y. The Conduct of Hostilities under the Law of International Armed Conflict. 3rd ed. – Cambridge : Cambridge University Press, 2016. – 354 p.
14. Pomson O. Methodology of identifying customary international law applicable to cyber activities // Leiden Journal of International Law. – 2023. – Vol. 36. – P. 1023–1047. DOI: 10.1017/S0922156523000390.
15. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135). – New York : United Nations, 2021. – 55 p.
16. Droit international appliqué aux opérations dans le cyberespace. – Paris : Ministère des Armées, 2019. – 18 p.
17. Application of International Law to States' Conduct in Cyberspace : United Kingdom Statement. – New York : United Kingdom Mission to the United Nations, 2021. – 18 p.
18. Huang Z., Ying Y. The Chinese approach to jus ad bellum in international law and cyberwarfare // The Cambridge Handbook of China and International Law / eds. I. Rasilla, C. Cai. – Cambridge : Cambridge University Press, 2024. – P. 203–218.
19. Лазарь К. К. Квалификация кибератак как «применения силы» или «акта агрессии» в международном праве: анализ статьи 51 Устава ООН и перспективы самообороны в киберпространстве // Правосудие/Justice. – 2025. – Т. 7, № 3. – С. 179–192. DOI: 10.37399/2686-9241.2025.3.179-192.
20. Schmitt M. N. Israel's Cautious Perspective on International Law in Cyberspace : Part I // EJIL:Talk! – 17 December 2020. – URL: https://www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-i-methodology-and-general-international-law/ (дата обращения: 20.05.2026).
21. Zetter K. Countdown to Zero Day : Stuxnet and the launch of the world's first digital weapon. – New York : Crown, 2015. – 448 p.
22. Roscini M. Cyber operations and the use of force in international law. – Oxford : Oxford University Press, 2014. – 301 p.
23. Батырь В. А. Ведение боевых действий в городах: правовые аспекты // Право в Вооружённых Силах. – 2022. – № 4 (297). – С. 12–27. EDN: WAMTOD.
24. Кудашкин А. В., Мельник Н. Н. Правовой режим специальных военных операций: сравнительно-правовой анализ // Право в Вооружённых Силах. – 2022. – № 4 (297). – С. 2–11. EDN: UKNPVJ.
25. Vestner T. The Law of Targeting's Mechanisation and Objectivisation through the Use of Artificial Intelligence // International Law and Technological Change : Testing the Adaptability of International Law / eds. I. Couzigou, E. Fromageau. – Cheltenham : Edward Elgar Publishing, 2025. – P. 211–234.
26. Non-International Armed Conflict in the Twenty-first Century / ed. by K. Watkin, A. J. Norris. – Newport : U.S. Naval War College, 2012. – 490 p. (International Law Studies ; Vol. 88).

Cyberattacks on Installations Containing Dangerous Forces: The Teleological Basis for the Applicability of the Article 56 Additional Protocol I Regime

Klimov Ya.I.

Financial University under the Government of the Russian Federation, M. M. Speransky Institute of Law and National Security, Russian Presidential Academy of National Economy and Public Administration

The article examines the normative basis for applying the special prohibition on attacks against installations containing dangerous forces (Article 56, Additional Protocol I to the Geneva Conventions of 1977, AP I) to cyberattacks on control systems of protected objects. Through teleological interpretation under Article 31(1) of the Vienna Convention on the Law of Treaties 1969, it is established that the prohibition in Article 56(1) AP I targets the consequence (release of dangerous forces) rather than the instrument, and therefore covers cyberattacks without any new treaty instrument. The ICRC functional approach (Report 32IC/15/11, 2015) and Rule 82 of the Tallinn Manual 2.0 confirm this conclusion. A comparative analysis of six states' positions reveals a structural asymmetry: states with the greatest cyber offensive capabilities have the least defined treaty obligations under Article 56 AP I. Three structural gaps are identified: textual (resolvable by teleological interpretation de lege lata), operational (requiring secondary instruments), and attribution (not amenable to interpretive resolution). Three complementary de lege ferenda measures are proposed with an assessment of their political feasibility.

Keywords: international humanitarian law, cyberattacks, teleological interpretation, installations containing dangerous forces, Tallinn Manual 2.0, attribution, *de lege ferenda*, ICRC, *opinio juris*, Stuxnet.

References

1. International humanitarian law and the challenges of contemporary armed conflicts: Report 32IC/15/11. Geneva: ICRC; 2015. 58 p.
2. Protection of civilians in armed conflict: Report of the Secretary-General (S/2020/366). New York: UN; 2020. 21 p.
3. Schmitt MN, editor. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge: Cambridge University Press; 2017. 598 p. DOI: 10.1017/9781316822524.

4. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I). Geneva, 08.06.1977. UN Treaty Series. Vol. 1125. No. 17512.
5. Vienna Convention on the Law of Treaties. Vienna, 23.05.1969. UN Treaty Series. Vol. 1155. No. 18232.
6. Sandoz Y, Swinarski C, Zimmermann B, editors. Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. Geneva: ICRC; Martinus Nijhoff; 1987. 1625 p.
7. Batyr VA. International legal protection of certain territorial objects during armed conflicts. Pravo v Vooruzhennykh Silakh. 2023;(8):44–55. (In Russ.). EDN: YXRUJX.
8. Henckaerts J-M, Doswald-Beck L, editors. Customary International Humanitarian Law. Vol. I: Rules. Cambridge: Cambridge University Press; ICRC; 2005. 621 p. DOI: 10.1017/CBO9780511804700.
9. HPCR Manual on International Law Applicable to Air and Missile Warfare. Cambridge: Cambridge University Press; 2013. 441 p. DOI: 10.1017/CBO9781139525275.
10. Biggio G. Regulating non-kinetic effects of cyber operations: the 'Loss of Functionality' approach and the military necessity-humanity balance under International Humanitarian Law. Journal of Conflict and Security Law. 2025;30(2):241–263. DOI: 10.1093/jcsl/kraf008.
11. Guidelines on the Protection of the Natural Environment in Armed Conflict. Geneva: ICRC; 2020. 128 p.
12. IHL and the Growing Involvement of Civilians in Cyber Operations. Geneva: ICRC; 2025.
13. Dinstein Y. The Conduct of Hostilities under the Law of International Armed Conflict. 3rd ed. Cambridge: Cambridge University Press; 2016. 354 p.
14. Pomson O. Methodology of identifying customary international law applicable to cyber activities. Leiden Journal of International Law. 2023;36:1023–1047. DOI: 10.1017/S0922156523000390.
15. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135). New York: United Nations; 2021. 55 p.
16. Droit international appliqué aux opérations dans le cyberespace. Paris: Ministère des Armées; 2019. 18 p.
17. Application of International Law to States' Conduct in Cyberspace: United Kingdom Statement. New York: United Kingdom Mission to the United Nations; 2021. 18 p.
18. Huang Z, Ying Y. The Chinese approach to jus ad bellum in international law and cyberwarfare. In: Rasilla I, Cai C, editors. The Cambridge Handbook of China and International Law. Cambridge: Cambridge University Press; 2024. P. 203–218.
19. Lazar KK. Qualification of cyberattacks as 'use of force' or 'act of aggression' in international law: an analysis of Article 51 of the UN Charter and prospects for self-defense in cyberspace. Pravosudie/Justice. 2025;7(3):179–192. (In Russ.). DOI: 10.37399/2686-9241.2025.3.179-192.
20. Schmitt MN. Israel's Cautious Perspective on International Law in Cyberspace: Part I. EJIL:Talk! 17 December 2020. Available at: https://www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-i-methodology-and-general-international-law/ (accessed 20.05.2026).
21. Zetter K. Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. New York: Crown; 2015. 448 p.
22. Roscini M. Cyber operations and the use of force in international law. Oxford: Oxford University Press; 2014. 301 p.
23. Batyr VA. Urban combat operations: legal aspects. Pravo v Vooruzhennykh Silakh. 2022;(4(297)):12–27. (In Russ.). EDN: WAMTOD.
24. Kudashkin AV, Melnik NN. The legal regime of special military operations: a comparative legal analysis. Pravo v Vooruzhennykh Silakh. 2022;(4(297)):2–11. (In Russ.). EDN: UKNPVJ.
25. Vestner T. The Law of Targeting's Mechanisation and Objectivisation through the Use of Artificial Intelligence. In: Couzigou I, Fromageau E, editors. International Law and Technological Change: Testing the Adaptability of International Law. Cheltenham: Edward Elgar Publishing; 2025. P. 211–234.
26. Watkin K, Norris AJ, editors. Non-International Armed Conflict in the Twenty-first Century. Newport: U.S. Naval War College; 2012. 490 p. (International Law Studies; Vol. 88).