Стрельцов Анатолий Александрович

заместитель директора Института проблем информационной безопасности
МГУ им. М.В.Ломоносова
доктор технических наук, доктор юридических наук, профессор

Применение международного гуманитарного права к вооруженным конфликтам в киберпространстве

Аннотация

В данной работе рассматриваются проблемы применения международного гуманитарного права к вооруженным конфликтам в киберпространстве. Раскрыто основное содержание термина «киберпространство». Рассмотрены содержание государственного суверенитета в киберпространстве и проблемы его реализации. Проанализированы проблемы применения международного гуманитарного права к вооруженным конфликтам в киберпространстве. Сформулированы предложения по направлениям адаптации и прогрессивного развития международного гуманитарного права применительно к выполнению гуманитарных задач в ходе вооруженных конфликтов в киберпространстве.

Ключевые слова

Международное гуманитарное право, вооруженные конфликты, киберпространство, информационно-коммуникационные технологии, государственный суверенитет, границы, методы и средства ведения войны, комбатанты, правовая защита, адаптация международного гуманитарного права.

1. Актуальность проблемы. В связи с активизацией разработки многими государствами методов и способов использования информационно-коммуникационных технологий (ИКТ) для решения задач военно-политического характера возрастает актуальность изучения вопросов применения международного гуманитарного права (МГП) к вооруженным конфликтам в киберпространстве. Как отмечено Группой правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности (2014-2015 гг.), «общее понимание применимости норм международного права к использованию ИКТ государствами имеет важное значение для содействия созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды» [1].

В рамках определения направлений реализации государственной политики Российской Федерации в области формирования системы международной информационной безопасности Президентом Российской

Федерации В.В.Путиным поставлена задача «содействия подготовке и принятию государствами – членами ООН международных актов, регламентирующих применение принципов и норм международного гуманитарного права в сфере использования ИКТ» [2].

Как отмечают специалисты [3], применение принципов и норм МГП (право Гааги и право Женевы) к вооруженным конфликтам в киберпространстве сопряжено с определёнными сложностями в трактовке этих принципов и норм. Данные сложности обусловлены, с одной стороны, новизной киберпространства как области применения МГП, а с другой - отсутствием универсальных международных договоров, регулирующих отношения в области использования ИКТ в качестве средства вооруженного насилия.

В качестве одного из возможных подходов к преодолению отмеченных сложностей некоторые специалисты предлагают воспользоваться международными обычаями [4-9]. При этом преодоление сложностей в трактовке международных обычаев применительно к вооруженным конфликтам в киберпространстве возлагается, по существу, на участвующие в конфликте стороны. Представляется, что при отсутствии всеобщей практики применения международных обычаев к рассматриваемым отношениям возникают условия для присвоения государством или группой государств права на принятие в ответ на злонамеренное использование ИКТ неких контрмер [10], несанкционированных Советом Безопасности ООН, а также для злоупотребления неотъемлемым правом на индивидуальную или коллективную самооборону, предусмотренным Статьей 51 Устава ООН.

В настоящей работе в развитие некоторых положений совместной работы А.В.Крутских и автора [11], рассмотрены: особенности киберпространства как сферы реализации государственного суверенитета; основные проблемы применения МГП к вооруженным конфликтам в киберпространстве; возможные направления адаптации и прогрессивного развития МГП для решения гуманитарных задач в ходе вооруженного конфликта в киберпространстве.

2. Киберпространство. В настоящее время не существует универсальной нормы-определения, закрепляющей понятие «киберпространство». В международных договорах Шанхайской Организации сотрудничества и некоторых двусторонних договорах Российской Федерации используется понятие «информационного пространства» как сферы деятельности, связанной с формированием, созданием, преобразованием, передачей, использованием, хранением информации и оказывающей воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию [12-14]. Данное понятие применительно к сфере инновационной деятельности раскрывается в межправительственном Соглашении Содружества Независимых Государств [15]. Так, в Соглашении «информационное пространство» трактуется как «совокупность информационных ресурсов, информационных систем и технологий,

информационно-коммуникационной инфраструктуры, обеспечивающих информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей». При этом «информационная инфраструктура инновационной деятельности» рассматривается как «множество юридических лиц, ресурсов, средств и других элементов, находящихся в отношениях и связях друг с другом, образующих целостность, направленную на обеспечение информационного обслуживания инновационной деятельности».

В свете изложенного для выполнения поставленной задачи представляется полезным согласиться с мнением группы российских и американских специалистов, занимавшихся изучением основ критически важной терминологии в области кибербезопасности [16]. По мнению данных специалистов, «киберпространство» является частью информационного пространства и представляет собой «электронную (включая фотоэлектронную и пр.) среду, в (посредством) которой информация создается, принимается, хранится, обрабатывается и уничтожается».

Как известно, электронная среда образуется совокупностью систем технических средств, обеспечивающих распространение электромагнитных волн по проводным и беспроводным каналам связи для передачи информации (средства связи и коммуникации), а также систем технических средств, обеспечивающих выполнение алгоритмов обработки информации (электронно-вычислительных машин), т.е. «технических средств и систем создания, преобразования, передачи, использования и хранения информации» образующих «информационную инфраструктуру» общества [12-14].

В российском законодательстве процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации, а также способы осуществления таких процессов и методов в электронной среде чаще всего объединяются термином «информационно-коммуникационные технологии» [17]. В англоязычной литературе этот термин трактуется в более общем смысле как понятие, интегрирующее все телекоммуникационные средства, компьютеры, а в случае необходимости - специальное и общее программное обеспечение, память, системы аудио-, видеовизуализации, используемые пользователем для накопления, передачи, обработки информации [18].

Исходя из изложенного, в киберпространстве выделяются три основные области верховенства государства:

электронная среда сбора, передачи, хранения и обработки информации, образуемая совокупностью сетей средств вычислительной техники, сетей средств связи и коммуникации и сетей средств хранения информации, расположенных на национальной территории;

ИКТ, определяющие методы и способы использования электронной среды для удовлетворения потребностей конкретного субъекта киберпространства (гражданина, организации, органа государственной власти, а также субъектов вооруженных конфликтов, а также преступных, в

том числе террористических, организаций), связанных со сбором, передачей, хранением, получением или распространением информации;

локальные или распределенные информационные системы, системы автоматизированного управления производствами и деятельностью людей.

Важной особенностью киберпространства является его глобальность, обеспечивающая возможность информационного взаимодействия людей и объектов, располагающихся на территории различных государств. Глобальность киберпространства достигается посредством соединения национальных электронных сред в единую электронную среду сбора, передачи, хранения и обработки информации на основе единой системы цифровой адресации субъектов и объектов киберпространства.

При отсутствии универсальных международных договоров международное правовое регулирование отношений в области системы цифровой адресации осуществляется на основе международных обычаев как всеобщей практики, признанной в качестве правовой нормы.

Один из таких обычаев заключается в выполнении американской неправительственной организацией Internet Corporation for Assigned Names and Numbers (ICAAN) деятельности по поддержанию и развитию системы распределения и использования цифрового адресного пространства (системы доменных имен). Данная система обеспечивает создание и поддержание в актуальном состоянии глобальное пространство цифровых адресов (доменных имен) субъектов и объектов глобального киберпространства. Это создает основу для использования ресурсов национальных киберпространств в целях выполнения ИКТ различных субъектов жизнедеятельности общества и государства.

Важным следствием применения рассматриваемого международного обычая для регулирования международных отношений является отсутствие в киберпространстве, в отличие от других, «традиционных» пространственных измерений государственного суверенитета национальных границ, а также международных соглашений о разделении адресного пространства между государствами и, соответственно, об их привязке к объектам информационной инфраструктуры, расположенным на национальных территориях. Данное обстоятельство во многом обусловлено тем, что организация ICANN не является международной межправительственной организацией и, следовательно, не является субъектом международного права. Соответственно, она не обладает ни международной правоспособностью, ни дееспособностью, ни деликтоспособностью.

Как известно, обеспечение функционирования системы цифрового адресного пространства (системы доменных имен) и обеспечение устойчивости этого процесса де-юре не относятся к области государственного суверенитета США и их международной правосубъектности в области киберпространства. Исходя из этого, можно констатировать отсутствие в системе международных отношений субъекта, несущего международную ответственность за выполнение функции обеспечения устойчивости глобального киберпространства к по отношению

к политическим рискам, существенно увеличившимся в современной системе международных отношений.

Существует и другое важное следствие применения рассматриваемого международного обычая к регулированию отношений в области поддержания единой системы цифровых адресов (доменных имен) в единой электронной среде. Оно заключается в том, что США де-факто распространили государственный суверенитет на регулирование вопросов обеспечения единства глобальной электронной среды, устойчивости соединения национальных электронных сред, а также информационного взаимодействия граждан различных государств, использования ресурсов национальных информационных инфраструктур для выполнения ИКТ в интересах субъектов различных сфер жизни общества. Одновременно другие государства мира не обладают возможностью реализации полного верховенства государства в национальном киберпространстве. Кроме того, существует неопределенность юрисдикции государств в вопросах контроля национальной электронной среды.

Не решает данную проблему и применение механизма обозначения государственных границ в киберпространстве посредством привязки объектов информационной инфраструктуры к национальной территории, предлагаемого некоторыми специалистами [8], т.к. не устраняет причины возникновения рассматриваемой проблемы.

Исходя из этого, можно отметить, что для выстраивания международных отношений в глобальном киберпространстве на основе принципа равенства суверенитетов, являющегося одним из важнейших принципов международного права, представляется целесообразным осуществить кодификацию норм, регулирующих международные отношения в глобальном киберпространстве.

3. Вооруженный конфликт в киберпространстве и применение МГП. Международный вооруженный конфликт и вооруженный конфликт немеждународного характера (далее – вооруженный конфликт) это, прежде всего, противоборство больших социальных групп населения, происходящее на территории нескольких государств или одного государства и в котором принимают участие вооруженные силы, а также могут принимать участие ополчение и добровольческие отряды, отвечающие определенным условиям [19].

Как известно, МГП представляет собой систему международно-правовых принципов и норм, регулирующих отношения между субъектами международного права в целях выполнения гуманитарных задач, возникающих в связи с вооруженными конфликтами [20]. Можно выделить несколько важных аспектов применения МГП к вооруженным конфликтам в киберпространстве:

территория, на которой осуществляется вооруженное противоборство;

методы и средства ведения вооружённого противоборства;

международно-правовой статус участников вооруженного конфликта;

правовая защита лиц и объектов в ходе вооруженного конфликта;

ответственность за нарушение МГП.

Рассмотрим выделенные аспекты применения МГП к вооруженным конфликтам в киберпространстве.

Территория вооруженного конфликта ограничивается территорией государства (государств), участвующих в этом конфликте [21]. Отграничение данной территории от территорий невоюющих государств осуществляется на основе международных договоров о государственных границах, заключаемых с соседними государствами по результатам делимитации границ. С этой точки зрения существование государственных границ позволяет принимать меры по локализации конфликта в границах противоборствующих государств.

Вооруженное противоборство в киберпространстве и, прежде всего, в глобальной электронной среде, позволяет оказывать «вооруженное воздействие» на любой объект, цифровой адрес которого имеется в едином пространстве цифровых адресов (доменных имен) независимо от их «привязки» к объектам информационных инфраструктур, расположенных на территории национальных государств. Отсутствие «карт привязки» объектов национальной информационной инфраструктуры к объектам инфраструктуры общества создает существенные трудности в соблюдении воюющими сторонами таких принципов МГП как различие гражданских и военных лиц; запрет нападения на лиц, не участвующих в военных действиях; запрет причинения излишних страданий; принцип пропорциональности; принцип необходимости; принцип гуманности. По этой же причине существуют существенные сложности в выполнении воюющими государствами международных обязательств по отношению к нейтральным государствам, равно как и в выполнении нейтральными государствами обязательств по отношению к участвующим к вооруженном конфликте государствам.

Важно отметить и то, что сложившаяся система сопровождения цифрового адресного пространства (системы доменных имен) предоставляет США весьма широкие возможности по манипулированию цифровым адресным пространством (доменных имен) национальных электронных сред государств, участвующих в вооруженном конфликте.

Важным аспектом международного правового регулирования отношений в области вооруженного конфликта является ограничение **методов и средств ведения вооруженной борьбы,** т.е. ограничение видов оружия, иных технических средств поражения противника, а также методов применения оружия и иных технических средств в ходе военных действий.

Как известно, термин «оружие» в обычном смысле слова представляет собой «всякое средство, приспособленное, технически пригодное для нападения или защиты, а также совокупность таких средств» [22]. Специалисты практически единодушно сходятся во мнении, что с правовой точки зрения ИКТ не являются оружием, равно как техническим средством вообще. В российской специальной литературе термин «ИКТ» часто рассматривается как синоним понятия «информационные технологии». Как

было отмечено выше, в российском законодательстве под «информационными технологиями» понимаются «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов» [17]. В англоязычной специальной литературе он трактуется в более общем смысле как понятие, интегрирующее все телекоммуникационные средства, компьютеры, а в случае необходимости - специальное и общее программное обеспечение, память, системы аудио-, видеовизуализации, используемые пользователем для накопления, передачи, обработки информации [18]. С этой точки зрения ИКТ не могут быть отнесены к «оружию», т.е. к средству (приспособлению), предназначенному для нанесения ущерба жизни и здоровью человека, или служить средством нападения на него и защиты.

Тем не менее, в региональных и двусторонних международных договорах Российской Федерации уже закреплен ряд понятий, отражающих опасения государств в связи с возможностью враждебного использования ИКТ для нанесения серьезного ущерба их национальным интересам. Так, в [12,13] введено понятие «информационного оружия», которое раскрывается как «информационные технологии, средства и методы, применяемые в целях ведения информационной войны». В свою очередь понятие «информационная война» трактуется как «противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны».

В международном договоре между Правительством Российской Федерации и Правительством Китайской Народной Республики [14] закреплено понятие «компьютерная атака», которое трактуется как «целенаправленное воздействие программными (программно-техническими) средствами на информационные системы, информационно-телекоммуникационные сети, сети электросвязи и автоматизированные системы управления технологическими процессами, осуществляемое в целях нарушения (прекращения) их функционирования и (или) нарушения безопасности обрабатываемой информации».

По мнению многих специалистов злонамеренное использование ИКТ способно нанести вред иногда сравнимый с применением традиционного оружия, а в ряде случаев – с применением оружия массового уничтожения [23], и, с этой точки зрения такое использование ИКТ представляет серьезную угрозу международному миру и безопасности и должно порождать неотъемлемое право государства на самооборону в смысле Статьи 51 Устава ООН.

Представляется, что ИКТ могут причинить подобный ущерб только в случае, если будут использованы для нарушения процессов и методов

управления средствами повышенной опасности, а также технологически опасными производствами, иными установками и сооружениями, содержащими опасные силы, нарушение правил управления которыми может привести к возникновению опасности тяжелых потерь среди гражданского населения, реальной угрозы жизни и здоровью людей, сохранению окружающей среды.

Возможность превращения обычных (неспециализированных) технических устройств в оружие вследствие нештатного их применения была использована террористами при осуществлении атак 11 сентября 2011 г. в США. Это обстоятельство при поддержке со стороны международного сообщества [24-27] позволило правительству США объявить о своем праве на индивидуальную и коллективную самооборону и начать вооруженные действия против Афганистана, обвиненного в поддержке террористов. Таким образом, террористическая атака 11 сентября 2001 г. с использованием захваченных террористами самолетов была де-факто приравнена к «вооруженному нападению» в смысле Статьи 51 Устава ООН. Очевидно, что данное решение несколько расширяет трактовку понятия «оружия», которая стала включать в себя устройства, которые при определенных обстоятельствах приобретают свойства «оружия». Такую разновидность оружия можно обозначить понятием «виртуальное оружие» [28].

К числу условий, при которых злонамеренное использование ИКТ превращает тот или иной объект или устройство в «виртуальное оружие», можно отнести:

способность наносить ущерб (поражение) живой силе и технике при нарушении нормального (штатного) режима их функционирования;

наличие в составе устройства или объекта информационных или коммуникационных систем, способных обеспечить реализацию акта злонамеренного использования ИКТ, приводящего к поражению живой силы и техники;

наличие ИКТ, предназначенной для превращения невоенного устройства или объекта в оружие.

В настоящее время не существует норм МГП, ограничивающих использование ИКТ в процессе вооруженного конфликта, несмотря на то, что их враждебное применение способно наносить повреждения, «имеющие чрезмерный характер», или оказывающее «неизбирательное воздействие».

Представляется, что на устранение данного недостатка не оказывает существенного влияния и предлагаемое некоторыми специалистами введение в правовое поле понятия «кибероперация», трактуемое как «применение кибермощностей для достижения основной задачи» [8]. По существу в данном определении речь идет об использовании электронной среды для выполнения ИКТ, способных наносить запланированный ущерб живой силе и технике. При этом существование ИКТ, предназначенных для достижения запланированной цели, подразумевается.

Важным аспектом МГП является определение **международно-правового статуса участников вооруженного конфликта**. В этой области

регулируются отношения, связанные с международно-правовым положением участников вооруженных сил и групп, представляющих стороны конфликта и являющихся субъектами применения оружия и иных технических средств в качестве средства вооруженного насилия.

Эти субъекты в соответствии с нормами международного права должны как минимум отвечать следующим условиям [29-31]:

иметь во главе лицо, ответственное за своих подчиненных;

открыто носить оружие;

соблюдать в своих действиях законы и обычаи войны.

Данные условия определяют правовые признаки комбатанта, имеющего право при определенных обстоятельствах рассчитывать на правовую защиту в соответствии с нормами МГП.

При применении данных норм МГП к участникам вооруженного конфликта в киберпространстве становится очевидно, что соблюдение комбатантами условия открытого ношения оружия, применяемого для осуществления вооруженного насилия, не представляется возможным. Более того, «виртуальный» характер ИКТ как средства ведения вооруженного противоборства позволяет государствам стимулировать участие в нем любых граждан, обладающих достаточной квалификацией и доступом к глобальной электронной среде и к объектам глобальной информационной инфраструктуры.

Таким образом, международно-правовой статус участников вооруженного конфликта в киберпространстве пока остается неопределенным.

Следующим аспектом применения МГП к вооруженным конфликтам в киберпространстве является **правовая защита лиц и объектов в ходе вооруженного конфликта**. Такая правовая защита посредством гарантированного предоставления определенного объема прав оказывается всем лицам, которые не принимают или перестали принимать непосредственное участие в военных действиях и оказались во власти неприятеля либо на территории вооруженного конфликта. К числу лиц, пользующихся такой правовой защитой относятся:

раненные, больные и лица, потерпевшие кораблекрушение;

военнопленные;

женщины;

дети;

журналисты;

гражданское население.

Общая правовая защита предоставляется МГП также гражданским объектам, в том числе критически важным объектам инфраструктуры, и культурным ценностям.

Соблюдение сторонами вооруженного конфликта, воюющими в киберпространстве, прав перечисленных лиц и обеспечение правовой защиты выделенных объектов во многом ограничено невозможностью их идентификации в электронной среде. Данное обстоятельство обусловлено

отсутствием международно-правового закрепления признаков объектов электронной среды и других объектов информационной инфраструктуры противостоящих государств, связанных с использованием гарантированных МГП прав или с предоставлением соответствующей правовой защиты.

Наконец, важным аспектом международно-правового регулирования отношений в области вооруженных конфликтов в киберпространстве является **ответственность за нарушение МГП.** В соответствии с международными договорами сторона, находящаяся в конфликте, нарушающая положения Женевских конвенций 1949 года или дополнительных протоколов к этим конвенциям [32], должна возместить причиненные убытки, если к этому есть основания. За нарушение норм МГП государство несет как политическую, так и материальную ответственность в форме реституции и компенсации [33].

Для проведения расследований любых фактов, которые, как предполагается, представляют собой серьезное нарушение, как оно определяется Конвенцией и Протоколом, или другое серьезное нарушение МГП, в соответствии с Дополнительным протоколом 1 к Женевским конвенциям 1949 года [34], создана Международная комиссия по установлению фактов.

Расследование нарушений МГП в киберпространстве сопряжено с необходимостью осуществления следующих действий:

выявление признаков нарушения МГП;

идентификация субъектов враждебного применения ИКТ в киберпространстве противоборствующих государств (государства), приведших к нарушению норм МГП;

выявление, фиксация и анализ электронных «следов» активности участников вооруженного конфликта в киберпространстве, причастных к нарушению МГП, а также обнаружение ИКТ, использование которой составляет объективную сторону международного правонарушения;

определение принадлежности субъектов враждебного применения ИКТ в киберпространстве к вооруженным силам государств, участвующих в вооруженном конфликте, или к антиправительственным вооруженным силам, другим организованным вооруженным группам, участвующим в конфликте;

классификация нарушений МГП и привлечение виновных лиц к установленной ответственности.

Выполнение Международной комиссией по установлению фактов перечисленных действий будет базироваться, прежде всего, на взаимодействии с субъектами обеспечения функционирования национальной информационной инфраструктуры, анализе информационных массивов информации, связанной с активностью субъектов применения информационных технологий.

Определенный опыт осуществления соответствующих оперативно-следственных действий в национальных киберпространствах уже накоплен национальными правоприменительными и правоохранительными органами

многих государств мира в рамках применения национального законодательства и региональных международно-правовых актов в области противодействия киберпреступлениям. В то же время возможность использования этого опыта в деятельности Международной комиссии по установлению фактов представляется весьма ограниченной. Это обусловлено в первую очередь незаинтересованностью государств, участвующих в вооруженном конфликте, в проведении таких исследований, в возможности манипулирования информацией, содержащей «следы» активности в киберпространстве как со стороны государств- участников конфликта, так и других заинтересованных государств.

4. Предложения. Можно выделить несколько направлений адаптации и прогрессивного развития принципов и норм МГП к киберпространству:

закрепление в международных договорах содержания государственного суверенитета в национальном киберпространстве, в том числе в области управления адресным пространством глобального киберпространства и его национального сегмента;

определение процедуры и проведение делимитации границ национальных киберпространств и закрепление границ этих пространств в соответствующих международных договорах;

определение объектов, включая критически важные, информационной инфраструктуры общества, пользующихся правовой защитой со стороны МГП;

создание и поддержание в актуальном состоянии «карт» привязки объектов национальной информационной инфраструктуры, которым предоставляется правовая защита МГП;

уточнение условий пользования международно-правовым статусом комбатанта лицами, осуществляющими акты враждебного использования ИКТ в качестве средства вооруженного насилия в составе вооруженных сил государств, других вооруженных групп, участвующих в вооруженном конфликте;

уточнение признаков враждебного использования ИКТ в качестве средства вооруженного насилия в отношении противника, лиц и объектов, защищаемых МГП;

совершенствование процедуры и условий исследования фактов нарушения МГП Международной комиссией по установлению фактов;

определение целесообразности создания международной системы объективизации событий, связанных с использованием ИКТ в ходе вооруженных конфликтов, для создания условий выполнения задач, возложенных на Международную комиссию по установлению фактов.

Закрепление соответствующих правовых новаций по каждому из выделенных направлений в универсальных международных договорах будет способствовать выполнению задачи обеспечения применимости норм международного права к использованию ИКТ на основе принципа суверенного равенства, укреплению общего понимания в целях повышения стабильности и безопасности в глобальном киберпространстве,

формированию единообразной практики применения МГП к вооруженным конфликтам в киберпространстве, а также методики оценки правомерности использования ИКТ в качестве средства вооруженного насилия в ходе военных действий в «традиционных» сферах применения вооруженных сил.

Список литературы

1. Доклад группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности. Представлен Генеральным Секретарем ООН 70-ой сессии Генеральной Ассамблеи ООН, 22 июля 2015 г., A\70\174.

2. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. 2013г. www.scrf.gov.ru/documents/6/114.html.

3. Proceeding of The Conference. International Expert Conference on Computer Network Attack and applicability of International Humanitarian Law. 17-19 November 2004. Stockholm, Sweden;

4. Российско-шведский научный семинар по международной информационной безопасности. 2 апреля 2013 г. Стокгольм, Швеция;

5. Восьмой международный научный форум "Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности", 21-24 апреля 2014 г., г. Гармиш-Партенкирхен, Германия;

6. International Engagement on Cyber: Developing International Forms for a Safe, Stable and Predictable Cyber Environment. 10 April 2013, Georgetown Journal of International Affairs. Washington DC (USA);

7. Российско-американская научная конференция «Управление Интернетом и киберконфликтами: модели, управление и меры укрепления доверия», 30 октября – 1 ноября 2013 г., г. Нью-Йорк (США).

8. Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual). M.Schmitt et al. eds. Cambridge University Press, forthcoming 2013; Katherina Ziolkowsky.

9. Peacetime regime for state activities in Cyberspace. International Law, International relations, Diplomacy. NATO CCD COE Publication. Tallinn. 2013.

10. Проект конвенции «Ответственность государств за международно-противоправные деяния». Резолюция Генеральной Ассамблеи ООН 56/83 от 12 декабря 2001 г.

11. Крутских А.В., Стрельцов А.А. Проблемы применения международного права к злонамеренному использованию ИКТ. Международная жизнь. 2014, 11.

12. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 16 июня 2009 года. Екатеринбург.

13. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности, 25 декабря 2013 года, Москва.

14. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности, 8 мая 2015 года, Москва.

15. Соглашение о создании инфраструктуры инновационной деятельности государств – участников СНГ в форме распределенной информационной системы и портала СНГ «Информация для инновационной деятельности государств – участников СНГ» Минск, 19 мая 2011 г. ст. 1.

16. Russia – US Bilateral on Cybersecurity. Critical Terminology foundations. EastWest Institute Worldwise Cybersecurity Initiative, Moscow state university information security institute. November 2013. http://wiki.informationsecurity.club/lib/exe/fetch.php?media=documents_all:russia-u_s_bilateral_on_terminology_rus.pdf

17. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ

18. en.wikipedia.org/wiki/Information_and_communications_technology

19. Женевская конвенция «Об улучшении участи раненных и больных в действующих армиях» от 12 августа 1949 г., ст.13.

20. К.А.Бекяшев. Международное гуманитарное право. В учеб. Международное право. Проспект, М., 2015, стр. 305.

21. Положение о законах и обычаях сухопутной войны. Гаага. 18 октября 1907 г. Отдел III.

22. Ожегов С.И.. Словарь русского языка. М., Русский язык. 1986, стр. 394;

23. Hoizington M., Cyberwarfare and the use of Force Giving Rise to the Right of self-Defense. 32 B.C. Int'l & Comp.L. Rev. 432 (2009), v. 32, Article 16.

24. Предварительный отчет 4370 заседания Совета Безопасности ООН от 12 сентября 2001 г.;

25. Предварительный отчет 4375 заседания Совета Безопасности ООН от 18 сентября 2001 г.;

26. Резолюция 1368 Совета Безопасности ООН от 12 сентября 2001 г.;

27. Резолюция 1373 Совета Безопасности от 28 сентября 2001 г. и другие.

28. Стрельцов А.А. Основные направления развития международного права вооруженных конфликтов применительно к киберпространству. Право и государство. 2014, №3.

29. Положение о законах и обычаях сухопутной войны. Приложение к Конвенции о законах и обычаях сухопутной войны. Гаага. 18 октября 1907 года. Ст.1;

30. Женевская конвенция «Об улучшении участи раненных и больных в действующих армиях» от 12 августа 1949 г., ст.13;

31. Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов, Женева, 8 июня 1977 г., ст.44.

32. Дополнительный протокол 1 к Женевским конвенциям 1949 года. 8 июня 1977 г. Ст.91.

33. Соколова Н.А. Международное гуманитарное право. В кн. Международное право. Отв. ред. К.А.Бекяшев. М., Проспект. 2015. Стр. 315.

34. Дополнительный протокол 1 к Женевским конвенциям 1949 года. 8 июня 1977 г. Ст. 90.