СЕТЕВЫЕ КОМПЬЮТЕРНЫЕ НАПАДЕНИЯ И СОВРЕМЕННОЕ МЕЖДУНАРОДНОЕ ПРАВО

А.Л. Козик

Международный университет МИТСО. 220099, Республика Беларусь, г. Минск, ул. Казинца, 21, корп. 3.

Проблематика сетевых компьютерных нападений (СКН) сегодня остра, как никогда. Использование государствами СКН для шпионажа, прекращения или приостановки деятельности компьютерных систем других государств и частных лиц стали реальностью. Государства действуют через своих агентов или привлекают для совершения атак группы наёмных хакеров. При этом вопрос о применимости международного права ни в доктринальном отношении, ни в практике окончательно не решён. Тем не менее существующий правовой режим (со всеми возможными его недостатками) обладает потенциалом для решения существующих проблем. Обязательства, взятые государствами по Уставу ООН и другим международным договорам, создают правовой режим, который невозможно игнорировать. Так, в зависимости от интенсивности характера последствий СКН могут являться или не являться нарушением запрета на применение силы (ст.2 Устава ООН), могут даже достичь порога вооружённого нападения, при котором государства получают право применить самооборону (ст.51 Устава ООН). Анализ существующего правового поля позволяет выявить пробелы и недостатки правового регулирования. Проблематика СКН довольно активно обсуждается в западной литературе, и это тем обиднее, что отечественная не уделяет ей должного внимания. В статье автор исследует проблематику сетевых компьютерных нападений, даёт их определение, анализирует юридический объём термина. Автор определяет те специфические черты СКН, которые представляют интерес с точки зрения современного международного публичного права.

Ключевые слова: сетевые компьютерные нападения, международное право, jus in bello; jus ad bellum, применение сил,; вооружённое нападение.

Компьютерные технологии, знакомые с рождения нашим детям, изменили мир. Сегодня микропроцессоры управляют всем – от истребителей до холодильников и телевизоров. Мы всё чаще сталкиваемся с тем, что информационные технологии бросают вызов установившемуся укладу, ускоряют нашу жизнь, ставят под сомнение эффективность существующего регулирования общественных отношений. Это неудивительно, ведь правовые формулы создавались без учёта того динамичного информационного обмена, который мы наблюдаем сегодня. Международные нормы, зафиксированные десятки лет назад, сегодня с трудом справляются с задачей регулирования вновь возникающих и существовавших ранее, но существенно изменившихся общественных отношений [12, с. 142–152; 13, с. 147–151].

Война, как наиболее масштабное по своему характеру и последствиям общественное явление, не стала исключением. Под влиянием развития информационных технологий понятие «поле боя» в буквальном смысле этого слова – как ограниченное пространство, на котором сталкиваются противоборствующие стороны, – утратило свой смысл. В современном вооружённом конфликте стороны всё больше опираются на новые средства и методы ведения войны, позволяющие уменьшить количество персонала в месте столкновения с неприятелем. Всё это влечёт изменения в понимании и оценке тех или иных деяний, в том числе общественно опасных.

Сетевые компьютерные нападения (СКН) уже давно находятся в поле зрения юристов-международников. Профессор Майкл Шмитт *(M.N. Schmitt)*, анализируя СКН, определяет его как не менее опасное оружие, нежели истребитель F-16, оснащённый высокоточным вооружением [36, с. 56]. Сетевые компьютерные нападения (СКН) – ситуации, в которых компьютерная сеть используется для совершения нападения на компьютерные системы с целью вывода их из строя или получения контроля над ними. К сожалению, в отечественной литературе в настоящее время нет ни одного исследования, касающегося проблематики СКН. При этом следует отметить, что своевременное правовое регулирование проблематики, связанной с информационными технологиями, не может не являться важной частью национальной безопасности страны [12, с. 142–152]. В США проблематике СКН отводится серьёзное место в военной доктрине [32; 33; 38].

Сетевые компьютерные нападения – термин, введённый в оборот в середине 90-х гг. прошлого столетия. В американской доктрине международного права СКН рассматриваются как часть «информационной войны», представляющей собой совокупность информационных операций (ИО). ИО определяются как действия, предпринимаемые для воздействия на информацию и информационные системы противника. СКН определяются как «действия, предпринимаемые путём использования компьютерной сети в целях нарушения *(disruption)*, отказа *(denial)*, ухудшения *(degradation)* или уничтожения *(destruction)* информации (доступа к ней), содержащейся в компьютерах и компьютерных сетях» [32, с. 113; 33, с. GL–9].

При этом в документах ВВС США можно найти следующие определения терминов:

– нарушение *(disruption)*: уменьшение возможности предоставлять или обрабатывать информацию; совокупность действий по задержке и уничтожению информации; отсрочка получения и распространения нового знания и уничтожение имеющихся знаний;

– прекращение *(denial)*: обратимая остановка информационного потока на определённое время;

– ухудшение *(degradation)*: постоянное уменьшение возможности предоставлять или обрабатывать информацию;

– уничтожение *(destruction)*: уничтожение информации до её передачи; необратимое уничтожение возможности предоставлять или получать информацию [38].

На наш взгляд, приведённый подход может быть справедливо подвергнут критике. Терминологический ряд составлен с нарушением логики, поскольку используемые термины логически пересекаются. Обобщив предлагаемые в науке определения, можно сделать вывод, что СКН обладает следующими характерными чертами:

1. Нападение осуществляется на компьютер[1] или компьютерную сеть[2].
2. В качестве инструмента нападения используется компьютер и характерная черта компьютеров – возможность взаимодействия в компьютерной сети.
3. Нападение представляет собой инициированный информационный обмен, использующий возможные технологические уязвимости в компьютере-жертве.

Однако если технические аспекты определения СКН не вызывают особых споров, то определение характеристик, присущих СКН как общественным отношениям, создаёт определённые трудности. Какие черты характерны СКН как общественным отношениям? Ответив на этот вопрос, мы сможем выделить те из них, которые подлежат правовому регулированию, поскольку подпадают под уже существующие правовые нормы; определить те, регулирование которых пока не осуществляется, но является желательным с точки зрения общественного бла-

[1] Под компьютером мы понимаем электронное устройство, способное принимать, обрабатывать и передавать информацию.

[2] Под компьютерной сетью мы понимаем систематизированную совокупность компьютеров, взаимодействующих друг с другом.

га или по иным причинам (конкретный подход здесь зависит от понятия, вкладываемого в термин «право») [5, с. 169–171; 8, с. 46]. Систематизировав эту информацию, то есть взглянув на СКН как на предмет международно-правового регулирования, мы сможем идентифицировать пробелы в международно-правовом регулировании и восполнить их, а также скорректировать практику правоприменения.

В современной науке ведётся дискуссия о категориях «общественные отношения» и «правоотношения» [10, с. 120–122; 17; 22]. Для целей настоящей статьи условимся, что специфическими чертами общественного отношения можно определить его содержание, отражающееся в объективной и субъективной стороне деяния, и субъектов. Рассматривая СКН, можно отметить, что субъектом этих общественных отношений выступают индивиды и правовые фикции – государства, юридические лица и проч.

Характеризуя объективную сторону, кроме уже указанных признаков (нападение осуществляется на компьютер или компьютерную сеть; в качестве инструмента нападения используется компьютер и возможность взаимодействия в компьютерной сети; нападение представляет собой инициированный информационный обмен, использующий возможные технологические уязвимости в компьютере-жертве) можно добавить, что СКН не охватывают ситуации физического уничтожения компьютеров – например, захват компьютерного зала (для последующей ясности будем именовать подобные нападения кинетическими в противовес кибернетическим нападениям).

С другой стороны, термин охватывает ситуации, при которых, хотя нападение и осуществлено на компьютер, его конечной целью является повреждение иной инфраструктуры, управляемой данным компьютером. Например, нападение на компьютер, управляющий светофорами с целью парализовать дорожное движение должно считаться сетевым компьютерным. СКН включает как действия нападающего путём воздействия на программную среду, так и использование запрограммированных микросхем, использование которых приводит к сбоям в работе систем (аппаратный уровень). Примером последнего является размещение поддельных микросхем в систему управления Транссибирским газопроводом. По утверждению некоторых авторов, последствием этой операции, проведённой ЦРУ США в 1982 г., стал трехкилотонный взрыв [27, с. 2].

Сегодня окружающая нас действительность такова, что практически в любом устройстве, потребляющем электричество, имеется компьютер. Большая часть компьютеров в свою очередь соединена в компьютерные сети. Это справедливо для персональных компьютеров, мобильных телефонов, уличных светофоров, видеокамер наружного наблюдения, систем контроля доступа, банкоматов и многих других предметов нашей жизни, ставших уже привычными [15]. Субъективная сторона СКН, как общественного отношения, включает в себя следующие элементы:

1. Вину в форме умысла.
2. Цель – контроль[3] или вывод компьютера из строя.

СКН может быть частью более масштабного плана действий и непосредственно вывод из строя или контроль над компьютером-жертвой может не являться конечной целью нападения. Именно конечная цель деяния зачастую является ключевым квалифицирующим признаком – именно этим отличаются, например, террористический акт (цель – запугивание, терроризирование населения) и иное посягательство на жизнь и личную неприкосновенность граждан. Однако для целей определения СКН как объекта исследования конечная цель не является существенной, хотя и может приниматься во внимание.

Любое ли СКН может и должно быть урегулировано правом? Иными словами, стать предметом правового регулирования? Ответ, как отмечено выше, зависит от понимания категории «право». Для нас очевидно, что право должно охватывать лишь те ситуации, в которых регулирование служит прямой общественной пользе. В первую очередь, путём защиты законных интересов субъектов. Так, например, не должны подлежать правовому регулированию ситуации, при которых субъект наносит вред самому себе или действует с согласия потерпевшего, деяния, при которых потенциальная общественная опасность и причиняемый вред отсутствуют или ничтожно малы и т.п.

При этом очевидно, что отдельные СКН могут быть, а иногда и должны быть подчинены правовому регулированию. В зависимости от субъектного состава и характера правового регулирования мы можем выделить два уровня правового регулирования СКН:

1. Уровень национальной системы права.
2. Уровень международной системы права.

Проблематика взаимодействия национальной и международной систем права достаточно подробно изучена в научной литературе [2; 3, с. 3-11; 4; 7; 9; 14, с. 170-180; 19, с. 3-8; 20]. Подчеркнём лишь, что нельзя рассматривать эти две системы как некую иерархию. Каждая из них имеет свой подход к регулированию общественных отношений, и поэтому они должны рассматриваться отдельно во взаимодействии. Анализ правового регулирования СКН на национальном уровне не входит в предмет исследования данной статьи, поэтому ограничимся лишь некоторыми важными для нас особенностями правового регулирования СКН на национальном уровне.

[3] Под контролем мы понимаем возможность управления компьютером-жертвой, то есть выполнение компьютером- жертвой последовательности команд, введённых нападающим.

При реализации государством уголовной и административной юрисдикции СКН выступает как элемент соответствующего правонарушения, имеющего, как правило, материальный состав (подразумевающий наступление последствий). При осуществлении гражданско-правовой юрисдикции государство обеспечивает гражданско-правовую защиту субъектов, чьи интересы нарушены сетевым компьютерным нападением. Особенностью СКН является то, что они могут осуществляться с использованием инфраструктуры компьютерных сетей, расположенных за пределами юрисдикции государства. Более того, абсолютное большинство СКН являются именно такими [12, с. 142–152; 13, с. 147–151]. Это приводит к объективной необходимости сотрудничества государств друг с другом. Такое сотрудничество может осуществляться только на основе международного права. Необходимость его обеспечения приводит к заключению международных договоров. Таким договором, криминализующим деяния, осуществляемые с использованием СКН, и обеспечивающим взаимодействие государств является, например, Конвенция о киберпреступности, принятая в рамках Совета Европы [6, с. 376–414].

Принятие подобных международных договоров является одним из примеров регулирования СКН на международно-правовом уровне. Однако в данном случае опосредуется связь государство–гражданин. Международное право выступает как способ усиления эффективности национальных правовых систем. Тем не менее международное право, и в этом его важная специфика, регулирует также общественные отношения, недоступные национальной системе права. Это отношения, в которых субъектами и адресатами предписаний выступают государства и международные организации. Правовая связь «государство–государство» может быть адаптирована только на международно-правовом уровне [14, с. 170–180]. Таким образом, можно выделить следующие ситуации, при которых СКН становится предметом международно-правового регулирования:

1. Как преступление (элемент преступления) международного характера.
2. Как деяние, за пределами регулирования *jus in bello*, присваиваемое, согласно международному праву, государству.
3. Как деяние в свете обязательств государств *jus in bello*.

СКН, как преступление или элемент преступления международного характера, некоторые авторы разделяют на киберпреступления и кибертерроризм [26, 25–70]. Киберпреступление – это общеуголовное деяние. Примером может служить мошенничество с применением СКН и его разновидности (кардинг, фишинг и проч.). Предметом международно-правового регулирования данные деяния становятся как следствие осознания государствами необходимости тесного сотрудничества в их раскрытии. Конвенция о киберпреступлениях налагает на государства-участники обязательства криминализировать, в частности, следующие деяния: несанкционированный доступ через Интернет, несанкционированный перехват интернет-данных, вред оборудованию интернет-систем, вмешательство в деятельность интернет-систем, интернет-мошенничество и подделки, производство и дистрибуция детской порнографии, нарушение авторских прав посредством Интернета [6, с. 376–414]. Первые четыре деяния, собственно, и представляют собой СКН. Это самостоятельные составы преступлений, криминализуемые впервые и неизвестные (с некоторыми оговорками, касающимися возможных аналогий) ранее. Иные деяния (мошенничество, производство детской порнографии, нарушение авторских прав) представляют собой ранее известные деяния, изменяется только способ их совершения.

Что касается кибертерроризма, то сам терроризм (с учётом возможных оговорок касательно применимости термина), хотя и является общеуголовным преступлением, однако после известных событий в Нью-Йорке и Мадриде международное сообщество выделяет его в особый ряд. Особая общественная опасность терроризма связана с общественным резонансом, который и является целью преступления. Терроризм сумел оформиться в самостоятельную силу, приобрёл международный характер и требует порой применения вооружённой силы для своего искоренения. Фактически террористический акт стал рассматриваться как jus ad bellum [21, с. 163–168].

Учитывая характерные особенности деяний и объективную необходимость сотрудничества государств, можно выделить правовые проблемы, требующие особого внимания:

– во-первых, требуется гармонизация подходов государств к определению составов правонарушений и ответственности за деяния. Отсутствие единого подхода затрудняет экстрадицию и иные формы сотрудничества. Указанная конвенция о киберпреступности важный, но, очевидно, недостаточный элемент такого взаимодействия;

– во-вторых, требуется создание более универсальных, нежели существующие, механизмов сотрудничества государств в вопросах оказания правовой помощи. Расследование трансграничных деяний возможно только посредством эффективного сотрудничества государств;

– в-третьих, требуется детальный анализ обязательств государств в области права прав человека относительно существующих в государствах механизмов и правовых возможностей по расследованию деяний, совершённых посредством СКН.

СКН как деяние за пределами регулирования jus in bello, присваиваемое, согласно международному праву, государству, выделяется тем, что выступает не просто как основание для ответственности государства, но в ряде случаев как противоправный акт с его стороны. Само

деление присваиваемых государству деяний на подпадающие под регулирование jus in bello и выходящие за его рамки следует устоявшейся в праве традиции и даже принципу международного права, согласно которому разделяют jus in bello и jus ad (contra) bellum [29, с. 613–624; 30, с. 267–201; 35, с. 157–196]. Таким образом, обязательства jus ad bellum являются одним из аспектов, подлежащих анализу применительно к отношениям связанным с СКН. Вслед за jus ad bellum следует выделить также иные деяния, не подпадающие под регулирование jus in bello и не касающиеся обязательств по применению силы, однако присваиваемые государству в соответствии с правом международной ответственности.

Обозначим здесь некоторые моменты, непосредственно связанные с СКН и требующие детального научного изучения:

– во-первых, подлежит выяснению, в каких случаях, учитывая специфику СКН как объекта исследования, нападение может быть присвоено («атрибутировано») государству;

– во-вторых, необходимо определить, является ли СКН применением силы. Одним из основных обязательств в современном международном праве является обязательство не применять силу или угрозу силой. Оно является общим и имеет характер обычая. Обязательство не применять силу и угрозу силой нашло отражение в ст. 2(4) Устава ООН. Сложность вопроса заключается в отсутствии единства среди учёных-международников в объёме категории «сила» в смысле ст. 2(4) Устава ООН. В советской доктрине международного права объём понятия довольно широк [16, с. 64–86; 18], в западной традиции он более узок и строго ограничивается вооружённой силой [1, с. 138–139] или вообще, в той или иной мере, отрицанием нормативной силы данного принципа [23, с. 809–837; 28, с. 509 – 613]. Ещё одним важным моментом является необходимость глубокого анализа СКН как общественного отношения и выделения в нём тех черт, которые позволили бы отнести его к категории применения силы, независимо от того, на основе какой из существующих доктрин строить дальнейшие умозаключения;

– в-третьих, если СКН можно считать применением силы, то будет ли оно считаться вооружённым нападением? В каких ситуациях применение СКН можно считать «инцидентом» или, например, «пограничным конфликтом»? Ответ на этот вопрос важен, поскольку определяет объём ответственности государства-инициатора и правовые возможности реагирования государства-жертвы;

– в-четвёртых, необходимо определить конкретные правовые возможности государства в случае совершения СКН против него. Существует ли правовая возможность задействовать положения ст. 51 Устава ООН (или ст. 5 Договора НАТО) и прибегнуть к самообороне? Вопрос также непрост, поскольку определение самообороны остаётся крайне неясным. За последние годы интерес к этому институту международного права возрос, однако противоречивая практика государств не позволяет считать дискуссию законченной. Особый интерес в этой связи вызывает возможность применения самообороны против негосударственных акторов;

– в-пятых, какова ответственность государства-инициатора СКН? Какие характерные черты СКН, возможно, создают специфику применения института ответственности в международном праве?

– в-шестых, несут ли ответственность государства-посредники, ведь, как правило, СКН осуществляется через инфраструктуру третьих государств. Каковы их обязанности по отношению к государству-инициатору и государству-жертве?

Данные вопросы не являются исчерпывающими. Необходимо подчеркнуть, что именно характерные черты СКН, и в частности особый способ осуществления – передача информационного потока через инфраструктуру множества государств, – представляют собой вызов нормам международного права, рассчитанным на регулирование главным образом «кинетических» отношений.

СКН в свете обязательств государств по jus in bello также вызывает особый интерес. В случае начала вооружённого конфликта, а также по ряду обязательств и в мирное время [11, с. 76–87], государства связаны положениями международного гуманитарного права. В ст. 1, общей для всех Женевских конвенций 1949 г., государства обязались «соблюдать и заставлять соблюдать конвенции»[4]. В связи с этим анализу должны быть подвергнуты любые ситуации, при которых использование СКН отличается от использования уже известных методов и средств ведения войны, а также соответствующие обязательства государств в мирное время. На наш взгляд, можно выделить следующие проблемные моменты:

– необходимо изучить механизм действия СКН и ответить на вопрос о том, является ли СКН методом или средством ведения войны. Это позволит определить, должно ли использование СКН подпадать под требования МГП к средствам и методам ведения войны;

– если СКН – средство или метод ведения войны, то очевидно, что государства, в силу положений ст. 36 Протокола I, должны осуществлять предварительную экспертизу (до принятия на вооружение) соответствующих технологий[5];

[4] Женевская конвенция об улучшении участи раненых и больных в действующих армиях. 1949 г. Москва, 2004.

[5] Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооружённых конфликтов (Протокол I). Женева, 8 июня 1977 года. (б.д.). Получено 11. 11. 2009 г. из http://www.icrc.org/Web/rus/siterus0.nsf/html/treaties-additional-protocol-1

– СКН основана на «информационном» воздействии на объект. Тем не менее предыдущий опыт человечества был основан на ведении кинетических, а не кибернетических войн. Положения Женевских конвенций 1949 г. и дополнительных протоколов могут не учитывать специфику «информационных войн». Необходим детальный анализ положений указанных документов для того, чтобы определить применимость норм МГП к СКН. Например, необходимо ответить на вопросы – кто является комбатантом в вооружённом конфликте с применением СКН, применим ли и в какой части институт непосредственного участия гражданского лица в военных действиях, обладает ли спецификой при СКН институт нейтральных держав, как обеспечить принцип различия и т.д.;

– необходимо решить гипотетический вопрос о том, что если конфликт между государствами ведётся исключительно с применением СКН, то, возможно, это не должно давать права государствам на использование кинетического оружия – по аналогии с *de facto* установившейся традицией не использовать ядерное оружие в ситуациях вооружённого конфликта с применением обычных вооружений.

Как видно из вышеизложенного, СКН является сложным предметом международно-правового анализа. Более того, такой анализ неизбежно будет носить комплексный характер. Международно-правовой анализ СКН позволяет выделить из объёма международно-правовых норм те, которые непосредственно затрагивают это социальное явление, определить уровень их эффективности, предоставляет возможность отыскать и восполнить лакуны в правовом регулировании СКН.

Ответ на вопрос о необходимости подобного исследования включает указание на необходимость обеспечения национальной безопасности, необходимость определения возможного поведения государства на международном уровне в случае вовлечения в ситуацию применения СКН, возможность более полно выполнить свои обязательства по международному гуманитарному праву.

Список литературы

1. Аречага де Э. Х. Современное международное право. М., 1983. 480 с.
2. Барбук А.В. Непосредственное применение норм международных договоров в национальных правовых системах. Дисс … к-та юрид. наук. Минск, 2005.
3. Барбук А.В. Соотношение международного и внутригосударственного права: теоретические аспекты // Журнал международного права и международных отношений. 2005. №1. С. 3–11.
4. Батлер У. Взаимодействие международного и национального права (на примере Великобритании) // Советское государство и право. 1987. № 5. С.112–118.
5. Вишневский А.Ф., Горбаток Н.А., Кучинский В.А. Общая теория государства и права: учеб. пособие (изд. 2-е, доп.). Минск, 2004. 639 с.
6. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Издательство «Юрлитинформ», 2002. С. 376–414.
7. Гаврилов В. В. Понятие и взаимодействие международной и национальных правовых систем. Владивосток: Издательство ДвГУ, 2005. 216 с.
8. Дробязко С.Г., Козлов В.С. Общая теория права: учеб. пособие для вузов. Минск, 2005. 464 с.
9. Зыбайло А. И. К вопросу о соотношении международного и национального права (теоретические аспекты) // Белорусский журнал международного права и международных отношений. 1998. №3. С.3–9.
10. Калинина Э. А., Козик А. Л. Общая теория государства и права. Краткий курс лекций. Минск: МИТСО, 2009. 198 с.
11. Козик А. Л. Действие норм международного гуманитарного права вне вооруженного конфликта. // Проблемы управления. 2006. №3 (20). С. 76-87.
12. Козик А. Л. Развитие информационных технологий и правовое регулирование общественных отношений // Studii Juridice Universitare. 2008. № 3-4. С. 142-152.
13. Козик А. Л. Трансграничность сети Интернет и связанные с ней проблемы международно-правового регулирования Интернет // Проблемы управления. 2008. № 2. С. 147-151.
14. Козик А. Л. Особенности международно-правовых отношений // Современные проблемы правовых отношений: сб. науч. тр. Минск: Академия МВД РБ, 2008. С. 170-180.
15. Компьютер - Википедия. [Электронный ресурс] Интернет-энциклопедия. Режим доступа: http://ru.wikipedia.org/wiki/Компьютер
16. Курс международного права: в 7 томах (Т. 2: основные принципы международного права). М., 1989. 239 с.
17. Кучинский В. А. Современное учение о правовых отношениях. Минск: Интегралполиграф, 2008. 317 с.
18. Менжинский В. И. Неприменение силы в международных отношениях. М., 1976. 295 с.
19. Павлова Л. В. Международное право в правовой системе государств // Белорусский журнал международного права и международных отношений. 1999. №3. С. 3-8.

20. Павлова Л. В., Бровка Ю. П., Чудаков М. Ф., Фадеев В. А., Леанович Е. Б., Зыбайло А. И. Имплементация норм международного права во внутригосударственное право. Минск: БГУ, 2001.147 с.
21. Павлова Л. В. Применимость обычных норм международного гуманитарного права в рамках борьбы с актами международного терроризма // Материалы международной конференции "Международное гуманитарное право: новые вызовы, новые испытания" (6-7 сентября 2007г., г. Минск). Минск: Министерство юстиции Республики Беларусь, 2008. С. 163-168.
22. Рыжов В. С. Общественные отношения: призрак и реальность // Право и политика. 2000. № 12.
23. Фрэнк Т. Who Killed Article 2(4)? Or: Changing Norms Governing the Use of Force by States. AJIL , 2005, Vol. 26 (№ 1). P. 809-837.
24. Шармазанашвилли Г. Самооборона в международном праве. М., 1973. 111 с.
25. Aldrich, R. W. How do you know you are at war in the information age. Houston Journal of International Law. 2000.
26. Brennen, S. W. Cyberthreats: The Emerging Fault Lines of the National State. Oxford University Press, 2009. 320 p.
27. Clark W. K., & Levin, P. L. Securing the Information Highway: How to Enhance the United States' Electronic Defenses. Foreign Affairs. Nov.-Dec. 2009. P. 2.
28. Coll J. A. The Limits of Global Consciousness and Legal Absolutism: Protecting International Law from Some of Its Best Friends. Harvard Journal of Internatonal Law , Vol. 27.
29. Gill T. The Nuclear Weapons Advsory Opinon of the International Court of Justice and the Fundamential Distinction Between the Jus ad Bellum and the Jus in Bello. Leiden Journal of International Law. 1999. № 12. P. 613-624.
30. Hongsheng S. The Evolution of Law of War. Chinese Journal of International Politics. 2006. Vol. 1. P. 267-301.
31. Joyner C. C., Lotrionte C. Information Warfare as International Coercion: Elements of a Legal Framework. EJIL. 2001. № 5. P. 825-865.
32. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02,12 April 2001 (As Amended Through 19 August 2009). URL: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf
33. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 3-13, Information Operations. URL: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf
34. O'Donnell B. T., & Kraska, J. C. Humanitarian Law: Developing International Rules For the Digital Battlfield. Journal of Conflict and Security Law. 2003. 8. P. 133-160.
35. Orakhelashvili A. Overlap and Convergence: The Interaction Between Jus ad Bellum and Jus in Bello. Journal of Conflict & Security Law . 2007. Vol. 12 (№ 2). P. 157-196.
36. Schmitt M. N. Computer Network Attack: the Normative Software. Yearbook of International Humanitarian Law. 2001. P. 53-85.
37. Schmitt, M. N., Harrison Dinniss, H. A., & Wingfield, T. C. Computers and War: the Legal Batlespace. Background Paper prepared for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law,Cambridge, June 25-27, 2004. 18 p.
38. USAF Intelegence Targeting Guide. United States Air Force Pamphlet 14-210, 1 February 1998. URL: http://www.fas.org/irp/doddir/usaf/afpam14-210/part11.htm#page88

Об авторе

Козик Андрей Леонидович – к.ю.н., доцент, заведующий кафедрой международного права Международного университета «МИТСО». Член Совета директоров Международного общества права войны и военного права (Брюссель), член Европейской ассоциации международного права (Флоренция), член международной уголовно-правовой сети (ICLN, Гаага), член Комиссии по имплементации международного гуманитарного права при Совете министров Республики Беларусь, член делегации Республики Беларусь в группе правительственных экспертов (GGE) ООН по вопросам информации и телекоммуникаций в контексте международной безопасности (2013). Республика Беларусь, г. Минск, ул. Казинца, 21, корп.3. E-mail: kozik_office@mitso.by

COMPUTER NETWORK ATTACKS AND MODERN INTERNATIONAL LAW

Andrey L. Kozik

International University MITSO, 220099, Belarus, Minsk, Kazintsa str., 21/3

Abstract: *Computer network attacks (CNA) is a no doubt actual theoretical and practical topic today. Espionage, public and private computer-systems disruptions committed by states have been a real life. States execute CNA's involving its agents or hiring private hacker groups. However, the application of lex lata remains unclear in practice and still undeveloped in doctrine. Nevertheless the international obligations, which states have accepted under the UN Charter and other treaties as well as customs – with any related exemptions and reservations – are still in force and create a legal framework, which one cannot ignore. Taking into account the intensity level or the consequences of a CNA the later could be considered as an unfriendly, but legal doing, or, as a use of force (prohibited under the article 2(4) of the UN Charter), or – in the case the proper threshold is taken – as an armed attack (which gives the victim-state the right to use force in self-defence under the customs and the article 51 of the UN Charter). Researches in the field of lex lata applicability to the CNAs could highlight gaps and week points of the nowadays legal regime. The subject is on agenda in western doctrine, and it is a pity – not in Russian one – the number of publication here is still unsatisfied.*

The article formulates issues related to CNAs and the modern international legal regime. The author explores the definition, legal volume of the term CNA, highlights main issues, which have to be analyzed from the point of the contemporary law.

Key words: Computer Network Attacks; CAN; International Law; jus in bello; jus ad bellum; use of force; armed attack.

References

1. Arechaga de E. Kh. 1983, Sovremennoe mezhdunarodnoe pravo [Modern International Law]. 480 s.
2. Barbuk A. V. Neposredstvennoe primenenie norm mezhdunarodnykh dogovorov v natsional'nykh pravovykh sistemakh. Kand. diss [Direct application of international treaties in national legal systems. Kand. diss]. Minsk., 2005.
3. Barbuk A. V., 2005, Sootnoshenie mezhdunarodnogo i vnutrigosudarstvennogo prava: teoreticheskie aspekty [The balance of international and domestic law: theoretical aspects], Zhurnal mezhdunarodnogo prava i mezhdunarodnykh otnoshenii [Journal of International Law and International Relations], Minsk. S. 3-11.
4. Batler U., 1987 Vzaimodeistvie mezhdunarodnogo i natsional'nogo prava (na primere Velikobritanii) [The interaction of international and national law (on UK example)], Sovetskoe gosudarstvo i pravo [Soviet State and Law], Moscow. S. 112-118.
5. Vishnevskii A. F., Gorbatok N. A., Kuchinskii V. A., 2004. Obshchaia teoriia gosudarstva i prava: uchebnoe posobie [General Theory of State and Law: Textbook]. 639 s.
6. Volevodz A.G., 2002. Protivodeistvie komp'iuternym prestupleniiam: pravovye osnovy mezhdunarodnogo sotrudnichestva [Counteraction to computer crime: the legal basis for international cooperation]. Moscow, Iurlitinform. S. 376-414.
7. Gavrilov V. V., 2005. Poniatie i vzaimodeistvie mezhdunarodnoi i natsional'nykh pravovykh system [The concept and the interaction of international and national legal systems]. Vladivostok, DvGU. 216 s.
8. Drobiazko S. G., Kozlov V. S., 2005. Obshchaia teoriia prava [General Theory of Law: Textbook]. Minsk. 464 s.
9. Zybailo A. I., 1998. K voprosu o sootnoshenii mezhdunarodnogo i natsional'nogo prava (teoreticheskie aspekty) [On the question of the relationship between international and national law (theoretical aspects)], Belorusskii zhurnal mezhdunarodnogo prava i mezhdunarodnykh otnoshenii [Belarusian Journal of International Law and International Relations]. S. 3-9.
10. Kalinina E. A., Kozik A. L., 2009. Obshchaia teoriia gosudarstva i prava. Kratkii kurs lektsii [General Theory of State and Law. A Short Course of Lectures]. Minsk, MITSO. 198 s.
11. Kozik A. L., 2006. Deistvie norm mezhdunarodnogo gumanitarnogo prava vne vooruzhennogo konflikta [Functioning of the International Humanitarian Law Beyond Armed Conflict], Problemy upravleniia [Problems of Government]. Minsk. S. 76-87.
12. Kozik A. L., 2008. Razvitie informatsionnykh tekhnologii i pravovoe regulirovanie obshchestvennykh otnoshenii [The Development of Information Technology and the Legal Regulation of Social Relations] Studii Juridice Universitare. Kishinev. S. 142-152.
13. Kozik A. L., 2008. Transgranichnost' seti Internet i sviazannye s nei problemy mezhdunarodno-pravovogo regulirovaniia Internet [Internet Transboundary and Related Issues of International Legal Regulation of the Internet], Problemy upravleniia [Problems of Government]. Minsk. S. 147-151.
14. Kozik A. L. Osobennosti mezhdunarodno-pravovykh otnoshenii [Features of International Legal Relations], Sovremennye problemy pravovykh otnoshenii: sbornik nauchnykh trudov [Modern Problems of Legal Relations: Collection of Scientific Works]. Minsk, Akademia MVD. S. 170-180.
15. Komp'iuter - Vikipediia. (2013). Available at: http://ru.wikipedia.org/wiki/Компьютер (accessed 5 October 2013).
16. Kurs mezhdunarodnogo prava: v 7 tomakh (Tom 2: osnovnye printsipy mezhdunarodnogo prava) [International Law Course: 7 Volumes (Volume 2: General Principles of International Law)]. Moscow. 1989. 239 s.

17. Kuchinskii V. A., 2008. Sovremennoe uchenie o pravovykh otnosheniiakh [The Modern Doctrine of Legal Relations]. Minsk, Integralpoligraf. 317 s.
18. Menzhinskii V. I., 1976. Neprimenenie sily v mezhdunarodnykh otnosheniiakh [Non-usage of Force in International Relations]. Moscow. 295 s.
19. Pavlova L. V., 1999. Mezhdunarodnoe pravo v pravovoi sisteme gosudarstv [International Law in the Jurisdiction of the States], Belorusskii zhurnal mezhdunarodnogo prava i mezhdunarodnykh otnoshenii [Belarusian Journal of International Law and International Relations]. Minsk. S. C. 3-8.
20. Pavlova L. V., Brovka Iu. P., Chudakov M. F., Fadeev V. A., Leanovich E. B., Zybailo A. I., 2001. Implementatsiia norm mezhdunarodnogo prava vo vnutrigosudarstvennoe pravo [Implementation of International Law Norms Into Domestic Law]. Minsk, BGU. 147 s.
21. Pavlova L. V. Primenimost' obychnykh norm mezhdunarodnogo gumanitranogo prava v ramkakh bor'by s aktami mezhdunarodnogo terrorizm [The Applicability of Customary Rules of International Humanitarian Law in the Fight Against Acts of International Terrorism], Materialy mezhdunarodnoi konferentsii "Mezhdunarodnoe gumanitarnoe pravo: novye vyzovy, novye ispytaniia" (6-7 sentiabria 2007g., g. Minsk) [Materials of the International Conference "International Humanitarian Law: New Challenges, New Test" (September 6-7, 2007., Minsk)]. Minsk. pp. 163-168.
22. Ryzhov V. S., 2000. Obshchestvennye otnosheniia: prizrak i real'nost' [Public Relations: The Specter and Reality], Pravo i politika [Law and Politics]. Moscow.
23. Frenk T. Who Killed Article 2(4)? Or: Changing Norms Governing the Use of Force by States. AJIL , 2005, Vol. 26 (№ 1). P. 809-837.
24. Sharmazanashvilli G., 1973. Samooborona v mezhdunarodnom prave [Self-defense in International Law]. Moscow. 111 s.
25. Aldrich, R. W. How do you know you are at war in the information age. Houston Journal of International Law. 2000.
26. Brennen, S. W. Cyberthreats: The Emerging Fault Lines of the National State. Oxford University Press, 2009. 320 p.
27. Clark W. K., & Levin, P. L. Securing the Information Highway: How to Enhance the United States' Electronic Defenses. Foreign Affairs. Nov.-Dec. 2009. P. 2.
28. Coll J. A. The Limits of Global Consciousness and Legal Absolutism: Protecting International Law from Some of Its Best Friends. Harvard Journal of Internatonal Law , Vol. 27.
29. Gill T. The Nuclear Weapons Advsory Opinon of the International Court of Justice and the Fundamential Distinction Between the Jus ad Bellum and the Jus in Bello. Leiden Journal of International Law. 1999. № 12. P. 613-624.
30. Hongsheng S. The Evolution of Law of War. Chinese Journal of International Politics. 2006. Vol. 1. P. 267-301.
31. Joyner C. C., Lotrionte C. Information Warfare as International Coercion: Elements of a Legal Framework. EJIL. 2001. № 5. P. 825-865.
32. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02,12 April 2001 (As Amended Through 19 August 2009). URL: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf
33. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 3-13, Information Operations. URL: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf
34. O'Donnell B. T., & Kraska, J. C. Humanitarian Law: Developing International Rules For the Digital Battlfield. Journal of Conflict and Security Law. 2003. 8. P. 133-160.
35. Orakhelashvili A. Overlap and Convergence: The Interaction Between Jus ad Bellum and Jus in Bello. Journal of Conflict & Security Law . 2007. Vol. 12 (№ 2). P. 157-196.
36. Schmitt M. N. Computer Network Attack: the Normative Software. Yearbook of International Humanitarian Law. 2001. P. 53-85.
37. Schmitt, M. N., Harrison Dinniss, H. A., & Wingfield, T. C. Computers and War: the Legal Batlespace. Background Paper prepared for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law,Cambridge, June 25-27, 2004.
38. USAF Intelegence Targeting Guide. United States Air Force Pamphlet 14-210, 1 February 1998. URL: http://www.fas.org/irp/doddir/usaf/afpam14-210/part11.htm#page88

About the author

Prof. **Andrey L. Kozik** –PhD in International Law (BSU), Head of the International Law Chair in International University "MITSO". Member of the Board of Directors of the International Society for Military Law and the Law of War, member of the European Association of International Law, member of the International Criminal Law Network, member of the National Governmental Commission for IHL Implementation, member of the Delegation to the Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (2013). Republic of Belarus, Minsk, 220099, Kazinza str, 21\3. E-mail: kozik_office@mitso.by.