Маркова Карина

студентка магистратуры двойного диплома МГИМО (У) МИД РФ и Свободного международного Университета социальных наук Гвидо Карли «Governance and Global Affairs»

Перевод статьи ***Вольфа фон-Хайнегга***

Международное право и международная информационная безопасность: ответ Крутских и Стрельцову

Статья 2014 года Андрея Крутских и Анатолия Стрельцова посвящена соотношению международной информационной безопасности и международного права. По всей видимости, целью статьи является продвижение идеи о новой правовой базе в сфере использования информационно-коммуникационных технологий (ИКТ), либо о необходимости значительной корректировки существующих принципов и правил, в частности тех, что касаются принципов *jus ad bellum* и *jus in bello*. Несмотря на то, что авторы подчеркивают необходимость соблюдения императивных норм Устава ООН, таких как невмешательство во внутренние дела государств и запрет на применение силы или угрозы силой, они исходят из предположения, что наблюдается «отсутствие полноценной международно-правовой базы, регулирующей деятельность государств в сфере использования ИКТ, в том числе и ее военные аспекты».

В поддержку своего призыва создать новую либо изменить существующую правовую базу, Крутских и Стрельцов задают 27 вопросов. К сожалению, им не

удается дается дать все ответы и часто они скорее запутывают, чем проясняют имеющиеся правовые вопросы. Интересно, что *Таллинское руководство*, которое представляется логичной и подходящей основой в дискуссии по применимости принципов *jus ad bellum* и *jus in bello* к кибероперациям, упоминается в статье, но ему не придается должного внимания.

Авторы придерживаются мнения, что *Таллинское руководство* является попыткой «натовских экспертов», «занимающих диаметрально противоположную позицию [политике России], направленной на предотвращение военно-политического противоборства в информационном пространстве», поскольку Россия «считает наивысшим приоритетом закрепление в системе международного права правил недопущения конфликтов из-за неправомерного использования ИКТ». Помимо того, что *Таллинское руководство* создавалось независимыми международными экспертами, а не «натовскими экспертами», сложно понять, почему авторы игнорируют его в целом, когда обсуждают, среди прочего, могут ли кибероперации расцениваться как «вооруженные нападения», инициирующие реализацию права государства на самооборону, и в какой степени. Трудно избежать ощущения, что авторы считают, что полные и подробные ответы, которые дает *Таллинское руководство*, в частности комментарий по поводу основополагающих принципов права, идут вразрез с их целью изменить международное право таким образом, чтобы это служило интересам Российской Федерации, что отличается от целей тех, кого авторы называют «Западом». Возможно, авторы статьи отвергают существующую правовую базу как несовершенную, потому что надеются, в конечном счете, на то, что будет наложен полный запрет на использование военной силы в киберпространстве.

Тем не менее, вопросы, которые задают авторы, и ответы, которые они дают, нельзя назвать неуместными, как и нельзя полностью ими пренебречь. Они рассматривают важные аспекты *jus ad bellum* и *jus in bello* и другие основные принципы международного права, такие как суверенитет. В основе их аргументов намеренно лежат существующие нормы международного права (*lex lata*). Таким образом, они придерживаются определенного понимания существующих принципов и правил международного права, что не должно оставаться без ответа. В этой публикации таллинского Центра киберзащиты НАТО анализируются некоторые вопросы и ответы с целью найти точки соприкосновения и расхождения.

Данная публикация не содержит ответа на вопросы 20, 24 или 26, как потому, что они не являются подлинными вопросами международного права, или потому, что авторы не смогли предложить никакого ответа. Вопрос 27 связан с возможной доработкой определения ИКТ с целью включить в него робототехнику и искусственный интеллект. Кажется, что таким образом авторы надеются поспособствовать очередному запрету на технологию, развитие которой находится в руках других стран, а не Российской Федерации. Вопрос 21 связан с усилиями, которые необходимо предпринять, чтобы предотвратить

использование ИКТ в террористических или криминальных целях. Ответ, который дается, практически ограничивается несогласием с Конвенцией Совета Европы по киберпреступности (Будапештская конвенция 2001 г.), что отражает опасения Российской Федерации. Авторы придерживаются точки зрения, что Будапештская конвенция не сочетается с принципом суверенитета, что может являться попыткой легализовать «глобальный шпионаж», и то, что в ней отсутствуют положения, касающиеся мер борьбы со спамом. Авторы предпочли бы принятие универсальной конвенции по киберпреступности, в которой были бы отражены эти опасения, что представляет собой очередную попытку расширить государственный контроль над киберпространством в большей степени, чем это необходимо для международной информационной безопасности, и угрожает экономическим и социальным преимуществам, которые несет свободное киберпространство.

Неправомерное использование ИКТ

Авторы используют выражение «неправомерное использование ИКТ» на протяжение всей статьи. То, что авторы характеризуют использование ИКТ в качестве «неправомерного», преждевременно, если по-прежнему рассматривать киберсредства в рамках международного права. В любом случае, непонятно, что авторы понимают под «неправомерным использованием» или о каких кибероперациях идет речь. Предположительно, это выражение используется по отношению к широкому кругу кибероперациий, которые совершаются государствами, и предполагает их несоответствие международному праву.

Адекватность существующей системы международного права

По всей видимости, вопрос 1 касается адекватности существующей системы международного права в сфере регулирования «неправомерного использования ИКТ», а ответ, который дается, не является полным. Естественно, сложно определить, можно ли квалифицировать кибероперацию как использование силы или вооруженное нападение согласно статьям 2 (4) и 51 Устава ООН соответственно. В этом отношении, несмотря на то, что предлагают авторы, «нарушение территориальных границ» пострадавшего государства не требуется, чтобы квалифицировать кибероперацию в этом ключе. Возможно, они подразумевают, что кибератака не обязательно проводит к материальному ущербу или к последствиям вне киберпространства, чтобы квалифицироваться подобным образом, или то, что «сила» может применяться удаленно, без физического вмешательства на территорию государства.

Если не принимать в расчет вопросы, касающиеся определений, общепризнано, что существующие принципы и правила международного права применимы к киберпространству и поведению государств в киберпространстве и с помощью него. Как правильно было отмечено в Консультативном заключении Международного суда по вопросу о ядерном оружии, «существующие принципы

и правила гуманитарного права … применимы ко всем видам военных действий и ко всем видам вооружения в прошлом, настоящем и будущем.

По всей видимости, практика государств подтвердила, что существующие принципы *jus ad bellum* и другие нормы международного права, в сущности, адекватны и их достаточно, чтобы регулировать поведение государств в киберпространстве. Тем не менее, государства должны продолжать сотрудничество в выработке консенсуса по поводу того, как эти принципы и правила должны применяться к киберпространству. Позиция авторов по этому вопросу неясна. С одной стороны, они выступают за применимость «вытекающих из Устава ООН общепризнанных принципов международного права *jus cogens»* к киберпространству. С другой стороны, они выступают, как минимум, за изменение существующих правил и, как максимум, за создание новой универсальной правовой базы, которая будет включать неуточненные аспекты контроля над вооружениями.

В этом отношении, необходимо прокомментировать вопрос 10. Он не обладает четкой формулировкой, но имеет отношение к квалификации кибероперaций в качестве террористических или криминальных. Авторы считают, что такая классификация позволяет пострадавшему государству отвечать на агрессию, не будучи ограниченным международным правом, даже если ответные меры могут нести угрозу международному миру и безопасности. Это неубедительный аргумент. Если ответные меры на криминальную или террористическую кибероперацию несут угрозу международному миру и безопасности, их нужно рассматривать в рамках *jus ad bellum*. Более того, в сферу применения международного права попадают любые ответные меры на криминальную или террористическую кибероперацию, которые затрагивает права и интересы других государств. Это так, даже если ответные меры, главным образом, направлены на негосударственного актора. В этом отношении, вышеупомянутые положения Устава ООН являются первостепенными.

***Jus ad Bellum:* квалификация кибероперaций как использование силы, акт агрессии или вооруженное нападение.**

Шесть вопросов – 2, 3, 4, 5, 6 и 11 – относятся к сфере *jus ad bellum*, то есть вопросов, когда кибероперация квалифицируется как использование силы, акт агрессии или вооруженное нападение.

Неубедительной представляется идея о том, как пишут авторы в ответе на вопрос 1, что «война, которая ведется в целях поражения противника, противоречит Уставу ООН, принципу суверенного равенства государств». Войны никогда не начинают, законно или противоправно, с целью проиграть. Это утверждение проливает свет на основной подход авторов к применимости принципов *jus ad bellum* к киберпространству, по всей видимости, который служит скорее цели предотвратить технологическую отсталость, чем содействовать укреплению международной (кибер) безопасности.

Судя по всему, подобный подход используется и в ответе на вопрос 3 по поводу применимости понятия «оружие» к ИКТ. В соответствии с Соглашением стран СНГ, авторы определяют «информационное оружие» как «информационные технологии, средства и методы, применяемые в целях ведения информационной войны». В отношении понятия «информационная война» они используют другое соглашение, по которому:

«… признаками информационной войны являются воздействие на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться перед лицом агрессора и не может воспользоваться законным правом самозащиты, нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах, компьютерные атаки на критически важные структуры».

Несмотря на бесспорную тенденцию среди государств все чаще включать кибероперации в такие понятия, как «использование силы» или даже «вооруженное нападение», до сих пор далеко не ясно, можно ли считать, что они должным образом отражают современное международное право. Более того, определение «информационной войны» ненадлежащим образом связано с потерей оборонных возможностей. Эта дискуссия демонстрирует, что понятие «информационная война» является слишком широким, чтобы способствовать прояснению того, насколько принципы *jus ad bellum* применимы к киберпространству, поэтому его следует избегать.

Вопрос 11 касается критически важной проблемы, состоящей в том, считаются ли кибероперации применением силы в соответствии со статьей 2 (4) Устава ООН. К сожалению, авторы не дают ответ на этот вопрос. Вместо этого они фокусируются на определениях «акта агрессии» и «вооруженного нападения».

Вопросы 2 и 4 связаны с определением «акта агрессии». В своем ответе на вопрос 2, авторы придерживаются позиции, что статья 2 резолюции «Определение агрессии» применима к кибероперациям, но «нуждается в адаптации с учетом специфики ИКТ», в частности, что касается отсутствия у некоторых из них кинетического эффекта. Это может быть так, но одновременно с этим не стоит забывать, что главная цель резолюции «Определение агрессии» состоит в том, чтобы дать руководящие указания Совету Безопасности ООН в определении наличия одного из условий, которые содержатся в статье 39 Устава ООН, для того, чтобы предпринять действия по поддержанию или восстановлению международного мира и безопасности. Вне всякого сомнения, данная резолюция зачастую принимается в расчет для того, чтобы определить имеет ли место вооруженное нападение, но тот факт, что Генеральная Ассамблея выработает новое определение агрессии, которое будет включать некоторые кибероперации, может стать опасным прецедентом. Международное право создается

государствами, они не должны отдавать эту прерогативу политическому по своей природе образованию, решения которого только в особых случаях будут приемлемы для сообщества всех стран. Более того, представляется сомнительным, что резолюция Генеральной Ассамблеи требует поправок. Как было продемонстрировано, в *Таллинском руководстве*, основополагающие определения принципов *jus ad bellum,* «использование силы» и «вооруженное нападение», могут быть интерпретированы в контексте киберпространства по существу и в свете последующих действий государств.

В то время, как вопрос 4 так же связан с понятием «акта агрессии», в его фокусе находится самооборона и понятие «вооруженного нападения». Праву на самооборону также уделяется внимание в вопросах 5 и 6. Авторы правильно подчеркивают, что, ввиду того, что у кибероперациий зачастую отсутствует кинетический эффект, их трудно квалифицировать как «вооруженное нападение». Следовательно, необходимо определить критерии, по которым кибероперации могут быть расценены как кинетическое вооруженное нападение. Тот факт, что авторы приводят пример «утечек секретной информации на сайте WikiLeaks» в этом контексте настораживает. Раскрытие органами иностранного государства секретной информации может рассматриваться как нарушение суверенитета, но не как использование силы или, тем более, как вооруженное нападение.

В своем ответе на вопрос 4 авторы также критикуют НАТО за распространение статьи 5 Вашингтонского договора на киберпространство. Они утверждают, то это решение «противоречит позиции стран НАТО о нецелесообразности разработки новых международных договоров в области информационных технологий и «автоматическом» применении существующих норм международного права». Из этого можно заключить, что авторы отрицают право других государств осуществлять свое суверенное право аутентично толковать статью 51 Устава ООН, несмотря на то, что по всей видимости, они оставляют это право за Содружеством Независимых Государств и Российской Федерацией. Помимо этого несоответствия подобная критика лишена оснований. Статья 5 Вашингтонского договора основывается на статье 51 Устава ООН и соответствующем действующем международном праве. Трудно понять, почему применимость права на самооборону в киберпространстве, которое ограничено по своему характеру и масштабу, не сочетается с пониманием того, что существующие нормы международного права подходят для регулирования поведения государств в киберпространстве и с помощью него.

По всей видимости, авторы не хотят признать применимость права на самооборону в случае кибероперациий, если только это не будет оговорено в международном договоре или на международной площадке, такой как Генеральная Ассамблея. Следовательно, в своем ответе на вопрос 5, (который, как и многие другие, касается права на самооборону), авторы придерживаются позиции, что Иран не может «подать в Международный суд жалобу на страны по обвинению их в организации атаки с использованием программы Stuxnet, ввиду

«отсутствия международно-правовой регламентации деятельности в данной сфере и соответствующих прецедентов». Возможно, авторы не готовы рассматривать атаку с использованием вируса «Стакснет» как вооруженное нападение в рамках статьи 51 Устава ООН. Так или иначе, осуществление права на самооборону не зависит ни от каких судебных разбирательств в Международном суде, что вызывает вопрос, почему это вообще упоминается. В конечном счете, авторы не дают ответ на этот вопрос. Им пошло бы на пользу ознакомиться с *Таллинским руководством* и объяснить свое согласие или несогласие с его положениями и комментариями по этому поводу, что было бы полезным вкладом в необходимую правовую дискуссию. В свою очередь, то, что делаются замечания и намеки, не представляется полезным.

Наконец, ответ на вопрос 6 по поводу предотвращения злоупотребления государствами права на самооборону в киберпространстве и в отношении него не способствует дискуссии. Авторы снова подчеркивают необходимость выработки «критериев обоснования оправданности и пропорциональности ответных действий». Поскольку это означает, что государства должны прийти к согласию по критериям того, можно ли считать кибероперации вооруженным нападением, авторы не должны подвергаться критике. Такие усилия без сомнения будут способствовать правовой ясности. Тем не менее, так же можно добавить, что более чем непонятно, готовы государства или нет договариваться по трактовке вооруженной кибератаки, выходящей за пределы статьи 51 Устава ООН. Подобная практика может стать плохим прецедентом, поскольку авторы отвергают любую трактовку вне какого-либо договора или международной платформы. Каждый раз, когда будет появляться новая технология, понадобится формальная трактовка, принятая методом консенсуса. Также невозможно обозначить определенные и объективные критерии для определения пропорциональности самообороны. Пропорциональность, как и раньше, будет зависеть от обстоятельств. Любая попытка поместить ее в рамки объективных и абсолютных критериев сведет это право на самооборону на нет.

Jus in Bello

Пять вопросов – 7, 8, 9, 16 и 17 касаются принципов *jus in bello*, попадающих под международное гуманитарное право или право вооруженных конфликтов. По всей видимости, закон о нейтральности рассматривается в вопросе 15.

Вопрос 17 относится к определению «театра военных действий» в киберпространстве. Авторы опять ограничиваются тем, что задают вопрос, но не дают на него ответ. Этот вопрос наводит на мысль о проблеме определения географических границ вооруженного конфликта и связанный с этим вопрос о географическом масштабе применения права вооруженных конфликтов. Неудивительно, что авторы не готовы занять какую-либо позицию, хотя при этом являются сторонниками демилитаризации киберпространства. Прояснение масштабов применимости права вооруженных конфликтов к киберпространству может идти в разрез с попытками, направленными на запрет его военного

использования. Тем не менее, такая демилитаризация, в какой форме она не проводилась бы, попросту недостижима в краткосрочной и среднесрочной перспективе. ИКТ используются вооруженными силами практически всех государств, и они осуществляют или планируют осуществлять операции в киберпространстве или с помощью него. Следовательно, киберпространство без сомнения является частью современного «театра военных действий», и, соответственно, право вооруженных конфликтов применимо к военным кибероперациями во время вооруженного конфликта. Другой вопрос состоит в том, может ли кибероперация сама по себе стать причиной вооруженного конфликта. Косвенно это находит отражение в вопросе 8, но он снова остается без ответа авторов.

Вопросы 7 и 8 касаются того, можно ли квалифицировать киберинфраструктуру врага в качестве правомерной военной цели, которую можно атаковать традиционными (кинетическими) вооруженными средствами (вопрос 7) или в качестве объекта, подпадающего под защиту права вооруженных конфликтов (вопрос 8), и что из этого следует. Авторы не дают ответа на первый вопрос, хотя он очевиден. В статье 52 (2) Дополнительного протокола I к четырем Женевским конвенциям 1977 г., который Российская Федерация ратифицировала 29 сентября 1989 г., дается определение правомерных военных целей. По всей видимости, отсутствие ответа снова связано с целью демилитаризовать киберпространство.

В своем ответе на вопрос 8, авторы придерживаются позиции, что «нормы международного гуманитарного права нуждаются в серьезной адаптации в связи с развитием ИКТ». Несмотря на то, что этот вопрос связан с киберинфраструктурой, которая находится на физическом уровне киберпространства, требование изменить существующее право вооруженных конфликтов оправдывается отсылкой к логическому уровню киберпространства. Тем не менее, что касается физической киберинфраструктуры, если ее не расценивать как военную цель, она подпадает под категорию гражданских объектов, находящихся под защитой от нападения. Авторы дают уклончивый ответ, что является следующим признаком того, что они не готовы признать применимость права вооруженных конфликтов к киберпространству.

Следовательно, представляется вполне логичным, что авторы не могут дать ответ на вопросы 9 и 16, которые связаны с принципами избирательности и пропорциональности. Несмотря на это, необходимо отметить, что эти основополагающие принципы права вооруженных конфликтов применимы к военным операциям в киберпространстве и с помощью него. В то время, как характеристики, присущие киберпространству, затрудняют определение правомерных целей или сводят к минимуму сопутствующий ущерб, эти сложности не освобождают участников конфликта от своих обязательств.

Неясно, как вопрос 15 отражает позиции нейтральных государств во время международного вооруженного конфликта. На первый взгляд, он связан с трудностями сохранения нейтрального статуса третьих государств, когда

стороны конфликта используют инфраструктуру, расположенную в третьих странах. Принимая во внимание последнюю часть вопроса, которая связывает такое использование с нарушением международного мира и безопасности, по-видимому, это понимание выходит за рамки закона о нейтралитете. Использование инфраструктуры нейтральных государств для осуществления прав вооруженной стороны, включая нападение, без сомнения является правовой проблемой. В этом смысле авторы правы. Тем не менее, то, что они просто подчеркивают существование трудностей, даже не дав элементарные ответы, не приносит никакой пользы. Отсылка к тому, как этот вопрос рассматривается в *Таллиннском руководстве*, опять же, была бы закономерной. Необходимо отметить, что государство не нарушает обязательств, который накладывает закон о нейтралитете, если не осуществляет постоянный мониторинг траффика данных, проходящего через его киберинфраструктуру. Нейтральное государство всего-навсего обязано прекратить вооруженные действия, о которых у него имеются сведения.

Атрибуция и ответственность государства

В фокусе вопросов 12, 13, 14 лежит проблематика атрибуции и ответственности. Согласно общепризнанным правилам права ответственности государств, действия государственных органов и частных акторов, которые уполномочены осуществлять деятельность под контролем государства, приписываются этому государству и могут вести к его международной ответственности. В своем ответе на вопросы 12, 14 авторы признают эти правила и подчеркивают существование практических трудностей в определении атрибуции в киберпространстве.

Интересно, что в вопросе 12 они утверждают, что использование территории третьего государства для проведения операций в киберпространстве, которое расценивается как неправомерное использование силы, может привести к приписыванию факта применения силы третьему государству, но «не перенесению на него ответственности за агрессию». Учитывая крайне категоричный характер этого суждения, оно является довольно проблематичным. Во-первых, самого факта того, что государство использует киберинфраструктуру третьего государства для неправомерных операций против другого государства, недостаточно для того, чтобы приписать осуществление кибероперации третьему государству. Последнее может нарушить свои международные обязательства, преднамеренно разрешив использование своей территории для совершения действий, которые ведут к серьезному ущербу в государстве, подвергшемуся нападению, или понести международную ответственность за содействие в операции, но факт прямого приписывания действий иностранному государству, как утверждается авторами, не находит отражения в современном международном праве.

Во-вторых, сложно понять различие, которое делают авторы, между атрибуцией применения силы и ответственностью за агрессию. Если использование силы, которое квалифицируется как акт агрессии, может быть приписано государству,

государство будет считаться ответственным за акт агрессии, за исключением тех случаев, когда оно ссылается на обстоятельства, исключающие противоправность, такие как право на коллективную самооборону. Естественно, возможно провести отличие между использованием силы и вооруженным нападением, но, если использование силы приводит к достаточно серьезным последствиям, чтобы расцениваться как вооруженное нападение, и, если его можно приписать третьему государству, право на самооборону пострадавшего государства будет распространяться не только на первое атакующее государство.

Ответственность третьих государств также рассматривается в вопросе 13, который посвящен ситуации, когда третье государство предоставляет свою инфраструктуру для использования в «противоправных целях». Авторы придерживаются точки зрения, что «необходима выработка международно-правовых норм, закрепляющих обязательства государства не допускать использование национального сегмента информационного пространства для совершения информационных атак со стороны другого государства против третьих стран». Было бы более чем удивительно, если бы авторы были не в курсе решения по Делу о проливе Корфу (*Corfu Channel*), в соответствии с которым государство обязано «не предоставлять намеренно свою территорию для совершения действий, нарушающих права других государств». Возникает вопрос, выступают ли авторы, тем не менее, за принятие новых правил международного права для киберпространства, поскольку они не удовлетворены существующими. В то время, как сами характеристики, присущие киберпространству, без сомнения ведут к новым проблемам, в частности, тем, что касаются идентификации и атрибуции, само по себе это не является причиной настаивать на принятии более строгих правил, чем существующие. С другой стороны, только сравнительно небольшое количество государств, возможно, включая Российскую Федерацию, обладают технологическими возможностями влиять и осуществлять мониторинг траффика данных, что обеспечило бы соблюдение предложенной правовой нормы. Для большинства государств существование более строгих стандартов, как в решении о проливе Корфу, было бы неприемлемым.

Государственный суверенитет

Проблема того, можно ли расценивать кибероперации как нарушение государственного суверенитета, рассматривается в вопросе 18. В частности, авторы задаются вопросом, «можно ли считать вмешательством во внутренние дела государства действия, направленные на получение несанкционированного доступа к почтовому ящику государственного лидера или высокопоставленного деятеля конкретной страны», «составляет ли это угрозу международному миру и безопасности, акт агрессии, подрыв государственного суверенитета». Авторы считают, что «противоправное использование ИКТ является подобной угрозой, только если представляет собой социально опасное деяние, повлекшее серьезные последствия национального или мирового масштаба».

В данном вопросе авторы оперируют разными понятиями международного права, которые нужно рассматривать отдельно. Не каждое нарушение суверенитета или вмешательство во внутренние дела государства может квалифицироваться как угроза международному миру и безопасности или акт агрессии. В то время как акт агрессии представляет собой угрозу международному миру и безопасности, второе понятие не ограничивается подобными действиями. Оно является гораздо более широким и подпадает под мандат Совета Безопасности ООН. Более того, действия в киберпространстве в самом деле можно рассматривать как нарушение суверенитета государства, подвергшегося нападению, даже если они не приводят к тяжким и серьезным последствиям, что авторы считают необходимым. Международное право не запрещает несанкционированный доступ к почтовому ящику лидера иностранного государства как акт шпионажа. Тем не менее, кибероперация, которая приводят к неправомерной узурпации ключевых суверенных прав государства, подвергшегося нападению, вполне может являться нарушением суверенитета государства, даже если это не привело к серьезным последствиям национального или мирового масштаба. В конечном счете, кибероперация будет расцениваться как нарушение суверенитета, если она приводит к последствиям национального или мирового масштаба. В таком случае, совокупный результат не важен.

По-видимому, вопрос 19 напрямую связан с принципом суверенитета.

«19. Какие международные либо национальные институты и на основании каких критериев уполномочены оценивать угрозы, возникающие в связи с противоправным использованием ИКТ в целях, представляющих угрозу международного миру и безопасности, а также последствия с точки зрения безопасности отдельных государств, нарушения их суверенитета, территориальной целостности и политической независимости?»

Ответ:

«Исходя из того, что правоприменением норм международного права в области международной безопасности занимается прежде всего государство, возникает озабоченность в связи с возможностью неадекватной оценки последствий и, как следствие, возникновением угрозы международной безопасности».

Можно только строить догадки по поводу значения вопроса и ответа, который дается. За исключением тех случаев, когда Совет Безопасности прибегает к своим полномочиям на основании главы VII Устава ООН, каждое государство без всякого сомнения имеет право определять есть ли угроза или факт нарушения его территориальной целостности или политической независимости. Оценить это всегда достаточно сложно, что влечет за собой возможность неправильного понимания, и может привести, в конечном счете, к угрозе международной безопасности. Следовательно, тяжело оценить практическую ценность вопроса и ответа, который на него дается. Авторы могли бы быть более конкретны,

например, обратив внимание на сложности, которые возникают, когда дело доходит до определения источника атаки, или на влияние, которое оказывается на государство, подвергшееся нападению.

Критическая инфраструктура

В вопросе 23 рассматривается важная тема – критическая информационная инфраструктура и ее защита от неправомерного вмешательства. Авторы делают отсылку к системам SCADA и другим системам, обеспечивающих работу, среди прочего, атомных электростанций и гидросооружений. Авторы предлагают официально запретить атаки на такие информационные инфраструктуры, что может быть достигнуто только после достижения договоренностей по критериям отнесения тех или иных объектов к категории критической информационной инфраструктуры. Они считают, что нельзя быстро и легко достичь необходимых договоренностей и рекомендуют, таким образом, придерживаться постепенного подхода, защитив, в качестве первоначальной меры банковскую инфраструктуру.

Естественно, что все государства, которые зависят от критических информационных инфраструктур, обеспокоены их уязвимостью. Следовательно, они усиливают меры по укреплению их отказоустойчивости и защиты. Тем не менее, все еще непонятно, вероятен ли процесс формализации защиты критических информационных инфраструктур и является ли он шагом в верном направлении. Во-первых, государства уже определи уязвимые стороны возможных противников, и многие обладают средствами, в том числе киберсредствами, чтобы нейтрализовать или вмешиваться в работу критической информационной инфраструктуры, если это кажется им правомерным и необходимым. Во-вторых, государства не согласятся на запрещение атак на такие инфраструктуры, если только это будет общепризнано и будет сопровождаться хорошо разработанным режимом проверки. В-третьих, создание режима проверки маловероятно, поскольку практически невозможно провести различие между «законными» и потенциально вредоносными киберсредствами. Наконец, призыв подписать международное соглашение по запрещению атак на критические информационные инфраструктуры может являться примером злого умысла, который нужно принять только после тщательного размышления.

Права человека

В соответствии с подходом Группы правительственных экспертов ООН в вопросе 22 авторы рассматривают необходимость «выработки норм, касающихся защиты прав человека и данных в информационном пространстве». Они делают прямую отсылку к правам человека, закрепленным в Международном пакте о гражданских и политических правах, включая ограничения, которые могут быть необходимы для защиты других прав человека или государственной безопасности, общественного порядка, здоровья или нравственности населения. Ввиду ситуации с правами человека во многих странах, необходимо рассматривать акцент на возможных ограничениях на свободу информации со

значительной степенью подозрения. Слишком часто государства берут на себя обязательства по защите прав человека, чтобы потом придерживаться их лишь на словах.

Заключительные замечания

Если в статье Андрея Крутских и Анатолия Стрельцова находит отражение официальная или полуофициальная позиция Российской Федерации по международно-правовым аспектам кибербезопасности, ее необходимо учитывать всем специалистам, работающим в данной области, будь то государственным служащим, научным работникам или всем заинтересованным в данной проблематике по другим причинам. Российская Федерация является и останется ключевым игроком в международных отношениях, и, следовательно, во всех вопросах, касающихся международной безопасности, включая кибербезопасность. Поскольку в статье рассматриваются вопросы, которые, по-видимому, важны для Российской Федерации, она является позитивным вкладом в идущую дискуссию по международно-правовым последствиям для кибербезопасности.

В то же время, многие положения и предложения, которые выдвигаются в статье, заслуживают значительной критики. В то время, как некоторые положения обоснованы и даже необходимы, слишком часто кажется, что авторами движет намерение использовать международное право как средство для компенсации технологической отсталости или для повышения государственного контроля над действиями в киберпространстве. Вероятно, что изменение или интерпретация международного права способом, предложенным в статье, будет служить интересам России, но необязательно интересам другим государств. Правила и принципы международного права, включая *jus ad bellum* и the *jus in bello*, в том виде, в котором они существуют на данный момент, не должны подвергаться изменению или трактовке, если это приводит к возможному подрыву международно-правовой стабильности.