ПРИМЕНЕНИЕ МЕЖДУНАРОДНОГО ПРАВА В КИБЕРПРОСТРАНСТВЕ

Ущерб, нанесенный частным лицам, организациям или объектам инфраструктуры в результате инцидентов в киберпространстве, в частности целенаправленных атак, может быть не менее существенным, чем последствия традиционных вооруженных конфликтов и столкновений. При этом в отличие от случаев применения традиционного кинетического оружия идентификация источника нападения при кибератаке крайне проблематична, а отсутствие международно-признанного определения акта агрессии в киберпространстве и общего понимания границы, за которой применение силы в нем может приравниваться к вооруженной атаке, оставляют обширное пространство для интерпретации намерений и действий сторон конфликта.

Старший советник по правовым вопросам Региональной делегации Международного Комитета Красного Креста (МККК) в Российской Федерации, Беларуси и Молдове Мария Станиславовна ***Гаврилова*** *(Россия), консультант ПИР-Центра Олег Викторович* ***Демидов*** *(Россия), генеральный секретарь Ассоциации международного права (Беларусь) Андрей Леонидович* ***Козик*** *и заместитель директора Института проблем информационной безопасности МГУ имени М. В. Ломоносова Анатолий Александрович* ***Стрельцов*** *(Россия) обсудили эти и другие вопросы на заседании круглого стола, состоявшегося в рамках 15-й Международной школы ПИР-Центра по проблемам глобальной безопасности.*

МАРИЯ ГАВРИЛОВА: Я буду говорить о регулировании киберпространства с точки зрения международного гуманитарного права (МГП) и возможности его применения в условиях вооруженных конфликтов, которые могут произойти с использованием информационных технологий, и постараюсь ответить на три вопроса:

- Почему Международный комитет Красного Креста (МККК) интересуется этой тематикой? Как взаимосвязаны Интернет и МККК?
- Как и в каком объеме МГП применяется в ситуации киберконфликта?
- С какими сложностями могут столкнуться органы государственной власти и эксперты при непосредственном применении МГП к киберпространству?

Позволю себе небольшую ремарку. МГП имеет две основные цели: ограничение средств и методов ведения войны во избежание лишних страданий мирного населения и защита гражданского населения и гражданских объектов, направленная на минимизацию материального и физического ущерба для лиц, не принимающих непосредственное участие в вооруженном конфликте.

МККК является хранителем МГП и, безусловно, заинтересован в его развитии. Даже если на данный момент мы не наблюдаем конфликтов в киберпространстве, можно предположить, что с развитием информационных технологий они будут играть все большую роль в вооруженных конфликтах. Таким образом, цель МККК — помогать развитию МГП, стремясь предотвратить, предусмотреть, урегулировать и, по возможности, предотвратить ситуации, которые потенциально могут нанести большой ущерб гражданскому населению.

Обращаясь к вопросу применимости МГП в киберпространстве, следует отметить, что большая часть его норм создавалась достаточно давно. В то время, когда мы и предположить не могли, что войны в киберпространстве возможны. Тогда это казалось научной фантастикой. Во многом именно с этим связаны споры о применимости МГП в киберпространстве. В самом деле, могли ли авторы международных договоров в 1949 и даже в 1977 г., которыми датируются основополагающие положения, потенциально подлежащие применению в ситуации киберконфликта, описать правила поведения, распространяющие свое действие на еще не существовавшее пространство?

Дополнительные сложности вызывает терминологическая путаница. Во-первых, как в средствах массовой информации, так и в научной литературе очень широко используется понятие *информационные войны*, которое смущает публику, потому что применяется оно не только к конфликтам, но и к пропаганде, работе СМИ и т. д. Безусловно, к информационным войнам, которые заключаются, например, в намеренной дезинформации населения в определенных политических целях, МГП не имеет никакого отношения. Оно применимо только к *классическим* вооруженным конфликтам, связанным с применением определенного рода силы. Хотя и тут есть свои особенности.

Киберконфликты, вне всяких сомнений, уникальны: во-первых, они не связаны с применением обычного, кинетического оружия, в связи с чем достаточно трудно определить место ведения боевых действий. Кибератаки могут происходить в разных точках планеты, находиться под юрисдикцией разных государств, и определить так называемый театр ведения военных действий, ограничить эту территорию порой бывает достаточно сложно.

Второй особенностью этих конфликтов является сложность, связанная с определением состава участников вооруженного конфликта. Для МГП крайне важно определить, кто именно принимает участие в военных действиях и от чьего имени. От этого зависят не только квалификация конфликта, но и более практические моменты, такие как объем защиты, предоставляемый каждому конкретного лицу, и определение законных целей для нападения. Также для МГП ключевое значение имеет определение лиц, ответственных за совершение военных преступлений, и привлечение последних к ответственности.

Но одно дело, когда вполне конкретные, официальные вооруженные силы вступают на территорию чужого государства, применяют на ней оружие, и совсем другое дело, когда мы говорим о хакерских конторах, ИТ-компаниях, разрушительное действие которых может быть не столь очевидно, а сами они могут быть рассредоточены по разным странам. Каким образом в такой ситуации осуществлять контроль, а в случае нарушений МГП выявлять виновных и привлекать к ответственности как государство, так и конкретных индивидов, непонятно. Все это накладывает особенности на применение МГП.

Тесно связан с этим вопрос безграничных возможностей негосударственных акторов. Все-таки в классических вооруженных конфликтах, к которым привычно применяется МГП, мы чаще всего говорим об армиях или о конкретных организованных вооруженных группах. В киберпространстве возможности негосударственных акторов, у которых просто есть доступ к компьютеру и соответствующее образование, значительно шире. Следовательно, мы можем столкнуться с ситуацией вооруженного конфликта, в котором будет принимать участие огромное число лиц, и контроль за всеми их действиями, привлечение их к ответственности станет непростой, если вообще посильной задачей.

Тем не менее, несмотря на то что киберконфликты представляют собой особые ситуации, в соответствии с уже сложившимся международным правом, что, в частности, было подтверждено консультативным решением Международного суда ООН, принципы МГП регулируют все виды, методы и средства ведения войны, которые когда-либо появлялись, существуют на данный момент или появятся в будущем. Также Группа правительственных экспертов ООН в своем последнем докладе отметила, что принцип гуманности — основа МГП — безусловно, применим к киберпространству. Осталось понять, с какими трудностями нам придется столкнуться, чтобы адаптировать МГП к новым реалиям.

Теперь о том, почему в этой тематике заинтересован МККК. Во-первых, в силу того что мы являемся хранителями МГП, мы заинтересованы в его развитии. Во-вторых, на данный момент огромное количество гражданской инфраструктуры, которая играет важную роль в жизни гражданского населения, опирается на компьютерные технологии. Если мы говорим о кибератаках, о киберконфликтах, то одни и те же сети могут использоваться как в военных так и в гражданских целях, в частности обеспечивать функционирование ядерных электростанций, госпиталей, и разрушение таких информационных систем может повлечь огромный ущерб для гражданского населения.

Одним из основных положений в МГП является четкое разделение гражданских и военных объектов. Когда мы имеем дело с киберпространством, когда один и тот же объект используется и в гражданских, и в военных целях, соблюсти это различие становится достаточно трудно. Например, та же GPS-навигация и банальный кабель может использоваться и в гражданских, и в военных целях.

МККК заинтересован в разработке новых или адаптации существующих норм для обеспечения более эффективной защиты гражданской инфраструктуры. В особенности, когда речь идет о защите объектов, необходимых для выживания гражданского населения, которые также могут пострадать в ходе конфликтов в киберпространстве, так как потенциально могут быть разрушены, например водоочистные сооружения.

Первые трудности, с которыми мы сталкиваемся при применении МГП, связаны с квалификацией вооруженного конфликта. Для того чтобы защита, предусмотренная МГП, распространилась на гражданское население конкретной территории, необходимо, во-первых, установить наличие вооруженного конфликта. Ситуация проще, когда в ходе вооруженного конфликта имеет место одновременное применение кинетического оружия и кибероружия. Намного сложнее установить наличие или отсутствие конфликта, когда мы имеем дело исключительно с кибератаками.

Существуют разные мнения и подходы относительно того, достаточно ли для начала применения МГП одних только кибератак. Ряд экспертов полагает, что не важно, какие методы ведения войны применяются — цифровые или кинетические. Сам факт начала применения этих методов и, как следствие, достижение определенного порога насилия, по мнению этих авторов, могут служить достаточным основанием для признания наличия вооруженного конфликта, к примеру, если при помощи кибероружия выводится из строя система навигации, в результате чего нарушается работа аэропортов, сталкиваются самолеты.

Есть и другое мнение на этот счет, которое состоит в том, что для кибероружия должен быть установлен более высокий порог интенсивности: такие операции должны проводиться постоянно, а ущерб от его применения должен быть значительным. Представляется, что это мнение не вполне основано на МГП, поскольку если мы говорим о международном вооруженном конфликте, то для его констатации достаточно и единичного случая применения силы, чтобы гражданское население получило предусмотренную договором защиту, а действия государств подлежали скрупулезной оценке на предмет соответствия критериям пропорциональности, соразмерности и иным ограничениям, о которых мы еще поговорим.

Как и в любой другой ситуации, связанной с применением силы, для киберконфликта принципиальное значение имеет квалификация его как международного или немеждународного. Если международный вооруженный конфликт, как было отмечено ранее, может состоять из единичного случая применения силы, то есть одной кибератаки, повлекшей за собой серьезные последствия, то для того, чтобы МГП начало защищать гражданское население от последствий кибератак, проводимых в ходе вооруженного конфликта немеждународного характера, необходимо преодоление определенного порога интенсивности, а в отдельных случаях — наличие организованной вооруженной группы. Если с интенсивностью все более-менее понятно, то установить участие в конфликте организованной вооруженной группы бывает не так просто.

Кроме того, от квалификации конфликта будет зависеть объем и содержание применимых норм. Часть положений МГП регулирует исключительно поведение участников классических международных конфликтов с участием государств. В случае же вооруженного конфликта немеждународного характера, где, по крайней мере, в роли одной из сторон выступает организованная вооруженная группа, круг применимых норм значительно уже, да и содержание отдельных требований может существенно отличаться. Именно поэтому анонимность в Интернете — это серьезная проблема для МГП.

Чтобы определить, какой блок норм применять, сначала нужно определить, кто воюет. В реальных боевых действиях это значительно проще — можно съездить и посмотреть на месте. Когда мы имеем дело с боевыми действиями с примене-

нием компьютерных технологий, далеко не всегда можно определить, откуда произошла атака, кто ее осуществлял, и уж тем более контролировалась ли она государством, с территории которого производилась, и в какой мере.

В данном случае нас спасает тот факт, что постепенно нормы обычного права восполняют пробелы в регулировании вооруженных конфликтов немеждународного характера и практически приравнивают две эти системы, в какой-то степени упрощая задачу защиты гражданского населения.

Какие положения регулируют вооруженные конфликты и защиту жертв в ситуации вооруженного конфликта? Во-первых, статья 36 Дополнительного протокола к Женевским Конвенциям. Эта норма является своеобразным ответом на критику в отношении МГП, которое якобы не адаптировано для кибероружия. В статье 36 говорится, что если государство разрабатывает новое оружие, не обязательно принимать новый договор или конвенцию, чтобы это оружие регулировалось МГП. МГП уже содержит ряд принципов, например пропорциональность, проведение различия, гуманность и т. д., которые регулируют применение любого вида оружия, независимо от того, когда оно появилось. И первое, с точки зрения МГП, что должно сделать государство, когда оно разрабатывает новое оружие, — это проверить его на соответствие МГП.

Также есть более общее положение, которое призывает государства обеспечить защиту гражданского населения и гражданских объектов. Это общая обязанность для атакующего и для защищающегося.

Сложности начинаются дальше, поскольку МГП содержит и более развернутые положения: запрет на нападение на объекты, необходимые для выживания гражданского населения; запрет на нападение на установки, содержащие опасные силы; принцип пропорциональности; меры предосторожности при нападении. Но для того чтобы эти нормы были применимы, необходимо установить факт нападения.

В рамках Дополнительного протокола к Женевским Конвенциям нападение определялось исходя из того, как это видели его создатели на момент принятия документа — а это 1977 г. Так, под нападением понимались «акты насилия в отношении противника, независимо от того, совершаются ли они при наступлении или при обороне». Однако практика пошла таким образом, что под актами насилия понимались в том числе военные операции, которые сами по себе используют ненасильственные методы без применения огня, но ведут к разрушениям и гибели гражданского населения. Таким образом, еще до возникновения вопроса о применимости МГП к кибератакам практика признала, что исходно ненасильственные методы в совокупности могут составлять нападения по смыслу договора.

В рамках *Таллинского руководства по международному праву, применимому при ведении кибервойны*, кибератака понимается как кибероперация, как наступательная, так и оборонительная, которая причиняет ранения или смерть людям либо ущерб объектам. С точки зрения МККК, не только ущерба и разрушения, но и нейтрализации объектов может быть достаточно, чтобы расценивать факт как нападение. Если обесточен, лишен возможности функционировать какой-то объект на АЭС, тот факт, что станция не разрушена, не говорит о том, что это не было нападением. Нейтрализован гражданский объект, что является достаточным основанием для применения МГП.

Один из важнейших для нас принципов — принцип пропорциональности, который означает, что ущерб гражданскому населению и гражданским объектам не может превышать то военное преимущество, которое сторона рассчитывает получить при помощи кибератаки. Самые большие трудности в данном случае возникают из-за тесной взаимосвязи гражданских и военных объектов, гражданской и военной инфраструктуры в киберпространстве. Военные объекты с точки зрения МГП — это те объекты, которые своим расположением, целью, использованием вносят эффективный вклад в военный успех государства.

Очень тяжело провести это разграничение в киберпространстве, когда, к примеру, GPS-навигация, компьютерные сети, Интернет работают как на гражданское население, так и на успех военной операции. Очень велик риск того, что гражданские объекты будут расценены как объекты двойного назначения и разрушены — в киберпространстве практически все будет являться объектом двойного назначения. Как в данном случае расценить эту пропорциональность, каким образом обезопасить гражданское население и посчитать, будет ли ущерб для гражданского населения перевешивать военное преимущество или нет?

Кроме того, от государства потребуется огромная техническая экспертиза, чтобы предвидеть и рассчитать, будет ли вообще нанесен какой бы то ни было ущерб. С точки зрения МГП это входит в обязанности государства — участника конфликта: просчитать ущерб, предусмотреть возможности для обратного пути, если станет ясно, что в ходе атаке пострадают гражданские объекты. Но намного проще дать указание остановить танк, который едет в город, чем остановить работу вирусов, которые уже были запущены в компьютерную систему, а результатом стало выведение объектов из строя.

Таким образом, несмотря на то что мы можем утвердительно говорить, что МГП регулирует киберконфликты, оно, очевидно, требует немалой доработки. Особую актуальность в контексте применения МГП в киберпространстве имеют следующие вопросы: противоречие между анонимностью в Интернете и необходимостью привлечения к индивидуальной уголовной ответственности за военные преступления, обязательство государства по обеспечению соблюдения МГП со стороны государств в условиях киберпространства, непосредственное участие в киберконфликтах и его возможные последствия для ИТ-компаний и иных возможных негосударственных участников боевых действий с применением компьютерных технологий.

ОЛЕГ ДЕМИДОВ: 22 июля 2015 г. был опубликован новый доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ ООН). Значение доклада, который стал плодом годовой работы уже четвертого по счету созыва Группы, история работы которой отсчитывается с 2001 г., состоит прежде всего в выработке свода политических норм, предлагаемых государствам — членам ООН в качестве первого шага к режиму ответственного поведения в киберпространстве.

Значение одиннадцати *добровольных и необязательных норм, правил или принципов ответственного поведения государств* уже стало предметом анализа в работах международных и российских экспертов, включая представителей ПИР-Центра. Выработка подобных правил, даже в качестве общих и сугубо добровольных предложений международному сообществу, стала значительным прогрессом как для

самой Группы, так и вообще для диалога об ответственном поведении государств в киберпространстве. Любопытно, что еще до публикации доклада деятельность ГПЭ стала ключевым предметом обсуждения на площадке 4-й Глобальной конференции по киберпространству, прошедшей в апреле 2015 г. в Гааге, Нидерланды.

Разворот западных дипломатов и экспертного сообщества, включая экспертов частного сектора, государственных и неправительственных научных центров, навстречу ГПЭ, проявившийся в Гааге, отразил две тенденции. Во-первых, сам дискурс о необходимости выработки норм поведения в киберпространстве для государств к 2015 г. окончательно утвердился, победил альтернативную точку зрения, согласно которой киберпространство по большому счету не нуждается в обязывающих нормах. Во-вторых, стало очевидно, что несмотря на хронические противоречия по ключевым вопросам между членами ГПЭ (прежде всего РФ и США) и ее неоднозначный для Запада имидж российской инициативы, служащей прежде всего интересам Москвы, работа Группы все же плодотворна и по большому счету безальтернативна. Последний факт легко объясним: ООН — единственная глобальная площадка, на которой имеет смысл договариваться об общих правилах для трансграничного киберпространства.

Однако росту внимания к работе ГПЭ во всем мире также послужило то, что с третьего созыва Группы в ее повестку была включена еще одна фундаментальная задача — адаптация к киберпространству существующих норм международного права, включая такие основополагающие его акты, как Устав ООН. В докладе ГПЭ 2013 г. было впервые заявлено, что Устав ООН применим и *имеет важное значение для поддержания мира и стабильности в киберпространстве*. Кроме того, в докладе отмечалось, что на поведение государств в киберпространстве и их юрисдикцию над ИКТ-инфраструктурой распространяются международные нормы и принципы, вытекающие из принципа государственного суверенитета.

Эти выводы Группы получили подтверждение и дальнейшее развитие в Докладе 2015 г. Кроме того, участникам ГПЭ удалось согласовать ряд мнений касательно вопроса о применимости международного права к киберпространству. Вкратце эти мнения включают:

- признание суверенитета государств над ИКТ-инфраструктурой в пределах их территории;
- необходимость соблюдения ряда международно-правовых принципов в киберпространстве (государственный суверенитет, суверенное равенство, мирное разрешение споров, невмешательство во внутренние дела);
- признание за государствами возможности принятия неуточненных мер в соответствии с Уставом ООН в контексте киберпространства;
- упоминание в контексте киберпространства ряда принципов (гуманности, необходимости, пропорциональности и индивидуализации);
- призыв отказаться от использования посредников (proxy actors) для противоправных действий в киберпространстве и от предоставления им своей территории;

- ответственность государств за противоправные действия в киберпространстве в случае, когда обвинения обоснованы и проведена надлежащая атрибуция таких действий.

Несмотря на свою безусловную важность, некоторые меры из этого списка все же можно назвать второстепенными, производными от первоочередных задач. Например, атрибуция кибератак с вовлечением государств имеет практический смысл только в том случае, когда определены и понятны возможные ответные меры в отношении автора противоправных действий в киберпространстве. Аналогично, целесообразность и сама возможность запрета на использование посредников для противоправных действий в киберпространстве определяется прежде всего тем, как международное сообщество будет квалифицировать действия с их участием, какие международно-правовые последствия эти действия будут создавать для причастных к ним государств (и самих посредников), и, опять же, какой диапазон ответных мер будет открыт для пострадавшей стороны в соответствии с общепринятой интерпретацией международного права.

Перенося эти тезисы на конкретный пример, вернемся к хорошо известной ситуации со *Stuxnet*. На сегодня мнение экспертного сообщества, подкрепленное техническим анализом кода червя, данными журналистского расследования Дэвида Сангера и заявлениями Эдварда Сноудена, почти не оставляет места для сомнений в том, что за созданием *Stuxnet* и его применением против объекта в Натанзе стоят американские и израильские спецслужбы. Представим, что уже в 2010 г. Ирану за счет привлечения внешних специалистов по информационной безопасности и организации трансграничного расследования инцидента удалось бы добыть технические свидетельства причастности АНБ и Моссада к операции по кибersаботажу иранских атомных объектов. Безусловно, в случае со *Stuxnet* речь идет о задаче исключительной сложности, однако сегодня атрибуция даже сложных целевых атак все же возможна при условии своевременных действий, сочетающих различные методы и техники. Но что Иран смог бы сделать с полученной информацией? И как международное сообщество в лице, например, Совета Безопасности ООН либо Генассамблеи ООН могло бы квалифицировать действия США и Израиля, даже получив от Ирана убедительные доказательства их причастности?

Этот же вопрос поднимали в своей статье, опубликованной в конце 2014 г., А. В. Крутских, известный в некоторых кругах как *киберцарь*, и один из ведущих отечественных экспертов по международной информационной безопасности (МИБ) А. А. Стрельцов. Кроме того, кейс *Stuxnet* рассматривается в *Таллинском руководстве* по применению международного права в условиях конфликта в киберпространстве CCD COE. Характерно, что ведущие эксперты и дипломаты России и стран НАТО не смогли дать ответа на этот вопрос — это невозможно до тех пор, пока не прояснена интерпретация ключевых понятий международного права применительно к киберпространству. Базовой *точкой отсчета* с точки зрения понятийного аппарата современного международного права, в свою очередь, является Устав ООН — наряду с конвенциями и другими актами, составляющими корпус международного гуманитарного права (jus in bello) и права вооруженного конфликта (jus ad bellum).

О каких конкретно понятиях идет речь? Их практически идентичный перечень приводят и российские авторы упомянутой статьи в журнале *Международная Жизнь*

и авторы Таллинского руководства. Выделим из этого перечня три наиболее важных понятия:

- угроза силой или применение силы (в соответствии со Статьей 2 (4) Устава ООН);
- акт агрессии (в соответствии со Статьей 39 Устава ООН);
- вооруженное нападение (в соответствии со Статьей 51 Устава ООН).

Важным *подспорьем* в вопросе о том, насколько вообще уместно применение этих понятий к действиям в киберпространстве, является Консультативное заключение Международного Суда ООН о законности применения или угрозы применения ядерного оружия в вооруженных конфликтах, 1996. В пункте 39 данного документа утверждается, что действие норм, прописанных в Статье 2 (4), Статье 42, Статье 51 и в целом в Главе VII Устава ООН, включая право государств на самооборону, не ограничено действиями с использованием какого-либо конкретного вида оружия. Таким образом, можно предположить, что с точки зрения Международного Суда ООН действие этих статей распространяется и на те ситуации в киберпространстве, когда ИКТ используются в качестве оружия. Однако здесь возникает новый терминологический вопрос: в каких случаях можно говорить об использовании оружия в киберпространстве. А. А. Стрельцов и А. В. Крутских указывают на разработанную терминологию *информационного оружия* и *информационной войны*, принятую как в доктринальных документах РФ, так и в международных договорах, таких как Екатеринбургское соглашение глав государств ШОС от 16 июня 2009 г. Однако за пределами ШОС, в том числе на площадке ГПЭ ООН, эти определения пока не используются.

В совокупности три приведенных выше понятия служат отправной точкой для того, чтобы так или иначе квалифицировать те или иные действия государств и посредников в киберпространстве, имеющие серьезные последствия (или создающие возможность для наступления таковых) для международной безопасности и/или международного мира. Возможность квалификации того или иного действия в киберпространстве также дает ответ на принципиальный вопрос о том, порождает ли такое действие у затронутого им государства право на самооборону в соответствии со Статьей 51 Устава ООН. В примере со *Stuxnet* основной вопрос звучит так: в случае наличия доказательств причастности США и Израиля к разработке и применению *Stuxnet* против иранских объектов следует ли считать эти действия применением силы, актом агрессии либо вооруженным нападением по смыслу соответствующих статей Устава ООН, и может ли Иран воспользоваться своим правом на самооборону? Ответ неизвестен именно в силу отсутствия общепринятой интерпретации Устава ООН для киберпространства.

В Таллинском руководстве предпринимается попытка выработать такую квалификацию, но в вопросе о *Stuxnet* группа экспертов не пришла к консенсусу. Согласно преобладающему мнению, кейс *Stuxnet* все же не может быть приравнен к применению силы, так как он не соответствует некоторым критериям, принятым экспертами CCD COE для квалификации действий в киберпространстве как применение силы. Перечень из 8 критериев приведен в правиле 11 Таллинского руководства, которое как раз посвящено определению понятия *применение силы* в киберпространстве. Ключевым критерием выступает серьезность последствий действия, которые могут проявляться в физических разрушениях инфраструктуры и иных

объектов, либо в человеческих жертвах, которые непосредственно повлекло действие в киберпространстве. Также используется ряд *качественных* критериев:

- мгновенный, незамедлительный характер действия;
- прямая, непосредственная связь между действием и последствиями;
- степень вторжения в чужое информационное пространство/ИКТ-инфраструктуру;
- измеримость последствий действия;
- военный характер действий;
- степень прямого вовлечения государства в кибероперацию/иное действие;
- наличие либо отсутствие прямого запрета на подобные действия в актах международного права.

В соответствии с этими критериями, даже если бы удалось доказать вовлечение США в создание и использование Stuxnet против Ирана, признать эту операцию использованием силы экспертам CCD COE помешал прежде всего тот факт, что ход и последствия были сильно растянуты во времени (как минимум 2008–2010 гг.). Кроме того, неизвестно, является ли с точки зрения экспертов Таллинского центра вывод из строя каскада центрифуг для обогащения урана в Натанзе достаточно серьезным разрушением для квалификации его как применения силы.

Следует заметить, что авторы Таллинского руководства взялись решать двойную по сложности задачу, так как понятие *применения силы* по смысле Статьи 2 (4) и вне контекста киберпространства не имеет точного определения. Что не менее важно, за прошедшие с момента принятия Устава ООН десятилетия не до конца прояснен вопрос о соотношении между собой понятий *применения силы*, *агрессии* и *вооруженного нападения*. Одной из ключевых ссылок в этом вопросе, которая также приводится в Таллинском руководстве, является решение Международного суда ООН от 27 июня 1986 г. по делу *О военной и военизированной деятельности в Никарагуа и против Никарагуа*, ответчиком по которому выступали США. Во-первых, в решении отмечается, что вооружение и подготовка США антиправительственных повстанческих группировок (контрас) представляет собой акт применения силы или ее угрозы в отношении Никарагуа.

Несмотря на то что это решение никак не связано с кибероперациями, оно достаточно важно в контексте сегодняшних задач, стоящих перед ГПЭ ООН и перед международным сообществом в целом. Во-первых, это означает, что применение силы не ограничивается прямым использованием вооруженных сил государства и может включать иные действия (вооружение, тренировка и пр.). Этот вывод актуален для киберпространства, так как кибероперации чаще всего весьма затруднительно рассматривать в качестве прямого использования национальных ВС. Кроме того, решение Международного Суда открывает возможность для квалификации как применения силы действий посредников (в данном случае отряды контрас), что также актуально для киберпространства.

Также решение МС ООН 1986 г. указывает на необходимость отграничения понятия *применения силы* от понятия *вооруженного нападения*: последнее включает *не все*, а лишь *наиболее серьезные* случаи применения силы. Этот принцип, очевидно, распространяется и на квалификацию кибероперациий с точки зрения

международного права. Вместе с тем ни текст решения, ни последующие документы Международного Суда ООН не сообщают четких критериев, которые позволили бы однозначно разграничить *применение силы* с *вооруженным нападением*. Соответственно, эта проблема будет автоматически переноситься и на квалификацию различных кибероперaций.

Наконец, не проясненным в рамках решения 1986 г. остается соотношение как применения силы, так и вооруженного нападения с понятием агрессии по смыслу Статьи 39 Устава ООН. При этом вне контекста соотношения с другими терминами из Устава ООН как раз понятию агрессии присуща наибольшая ясность. Определению агрессии посвящена отдельная одноименная резолюция Генассамблеи ООН № 3314 от 4 декабря 1974 года. В Статье 3 резолюции приводится перечень из семи видов действий, подпадающих под понятие агрессии. В резолюции отмечается, что список не является исчерпывающим и может быть пополнен решением Совбеза ООН. В настоящее время эта опция приобретает растущую актуальность, так как документ, принятый 41 год назад, по понятным причинам не говорит ничего о действиях с использованием ИКТ и агрессии в контексте киберпространства. Подробный анализ Резолюции производит в своей недавней работе коллектив авторов Минобороны РФ. При этом военные эксперты МО РФ продвигают идею не обновления текста резолюции, а его адаптированного прочтения, которое охватывало бы операции в киберпространстве, потенциально подпадающие под понятие агрессии. В частности предлагается рассматривать использование одним государством прокси-серверов на территории второго для атак на третье как действие, подпадающие под пункт *f)* Статьи 3 Резолюции (предоставление государством своей территории для совершения актов агрессии в отношении третьего государства). Также рассматривается интерпретация применительно к действиям хакерских групп-посредников пункта *g)* (засылка государством или от имени государства вооруженных банд, групп, иррегулярных сил или наемников, осуществляющих применение вооруженной силы).

Однако авторы работы признают, что ключевым недостатком Резолюции ГА ООН является отсутствие у нее обязывающей силы. Следовательно, заложенное в ней определение агрессии, даже при наличии его консенсусной интерпретации применительно к кибероперациям, вряд ли сможет служить прочной основой международно-правового режима в этой сфере. В этой связи любопытная опция предлагалась тем же авторским коллективом МО РФ ранее: инкорпорировать определение агрессии, адаптированное к киберпространству, в Римский Статут Международного уголовного суда (МУС). В 2011 г. на конференции по обзору Римского Статута МУС была принята резолюция о включении в Статут понятия *преступление агрессии*, взятого из Резолюции № 3314 ГА ООН. Но фактическое осуществление юрисдикции МУС по этому преступлению станет возможно только в случае принятия соответствующего решения на следующей обзорной конференции по Римскому Статуту МУС, проведение которой запланировано на январь 2017 г. На данный момент существует вероятность того, что принятие решения может быть отложено и на более дальнюю перспективу. С одной стороны, это дает возможность начать и развить широкую международную дискуссию об адаптации текста Резолюции № 3314 (и параллельно понятия *преступление агрессии* в Римском Статуте МУС) к кибероперациям. В том числе вероятной площадкой для такой дискуссии видится как раз ГПЭ ООН, следующий, пятый созыв которой должен начать свою

работу в 2016 г. С другой стороны, даже в случае достижения компромисса по этому вопросу в рамках ГПЭ ООН временные перспективы вступления в силу обязательного определения агрессии, адаптированного к кибероперациям, — в рамках юрисдикции МУС или в ином формате — пока неясны.

В свете рассмотренных выше терминологических коллизий важен вопрос о том, возьмется ли следующий созыв ГПЭ ООН решать их. Участники группы, включая российских дипломатов, неоднократно делали акцент на том, что мандат Группы не включает глубокую ревизию норм международного права с целью их адаптации к киберпространству — задача ГПЭ состоит в выработке более общих и практических норм поведения в этой сфере. Однако логика подсказывает, что полностью скинуть с себя эту функцию Группе не удастся по нескольким причинам. Во-первых, дальнейшее расширение и даже простое поддержание консенсуса между членами Группы невозможны без общего понимания ключевых терминов, на которые опираются выработанные Группой нормы поведения. В том числе речь идет и о терминах из Устава ООН.

Во-вторых, ставки растут: чем дольше Группа избегает тяжелой и кропотливой работы по глубинной интерпретации основополагающих норм международного права применительно к киберпространству, тем больше шансов на то, что на практике военно-политический курс ведущих держав в сфере кибероперациий будет опираться на видение международного права, сформулированное в рамках других площадок либо выработанное самостоятельно и вообще ни с кем не согласованное.

Отчасти этот процесс уже происходит. Опыт и выводы, полученные в ходе работы над Таллинским руководством, несмотря на его сугубо экспертный статус, уже находят отражение в реальной политике НАТО. В сентябре 2014 г. в ходе саммита НАТО в Уэльсе прошел обзор Углубленной доктрины кибероборонь Организации. По его итогам было принято политическое решение о том, что право членов НАТО на коллективную оборону, заложенное в Статье 5 Вашингтонского договора, распространяется и на те случаи, когда государство — член НАТО становится жертвой нападения в киберпространстве. Отныне кибератака на страну — члена НАТО, повлекшая гибель людей или масштабное разрушение инфраструктуры, и, по мнению Организации, совершенная напрямую государством или его посредниками, может повлечь вооруженный ответ НАТО с использованием всего доступного ей военного потенциала, не ограничиваясь киберпространством. При этом вопрос об атрибуции кибератаки, способной запустить механизм коллективной обороны, будет решаться военным командованием НАТО по ситуации в каждом конкретном случае. Потенциальные риски такого подхода хорошо иллюстрируются примером 2007 г., когда Эстония, ставшая жертвой мощной волны кибератак в разгар так называемого *кризиса Бронзового солдата,* запросила руководство НАТО о возможности применения Статьи 5. При этом в качестве агрессора рассматривалась РФ, которую Эстония обвинила в организации и осуществлении кибератак, несмотря на отсутствие надежных доказательств. Повторись такая ситуация сегодня, с учетом новой доктрины кибероборонь НАТО речь могла бы идти о потенциальной эскалации кризиса между Россией и НАТО.

Стоит отдельно отметить развитие взглядов США на международно-правовую сторону кибероперациий. В июне 2015 г. было опубликовано свежее издание Руководства Министерства обороны США по праву войны (DoD Law of War Manual).

Публикация содержит отдельную главу, посвященную кибероперациям, где среди прочего четко прописаны критерии и условия, при которых кибероперация квалифицируется как незаконное применение силы по смыслу Статьи 2 (4) Устава ООН. В Руководстве приводятся три примера таких операций:

- кибероперация, которая вызывает мелтдаун реактора АЭС;
- кибероперация, которая вызывает открытие дамбы ГЭС в густонаселенной местности, ведущее к человеческим жертвам;
- кибероперация, которая нарушает работу авиадиспетчерских служб, что в свою очередь ведет к авиакатастрофе.

Дополнительно в документе упоминаются и иные примеры кибероперций, которые могут быть признаны актами применения силы, включая операции, нарушающие работу систем военной логистики и в результате препятствующие планированию военных операций и управлению войсками.

Несмотря на то что Руководство не является источником права и не имеет никакой юридической силы, его положения служат практической инструкцией для служащих Вооруженных сил США, включая, например, такие структуры, как Объединенное киберкомандование ВС США.

Для международного сообщества риск разноскоростной, нескоординированной деятельности различных государств и региональных альянсов по выработке интерпретации международного права применительно к киберпространству состоит в том, что в отсутствие общей площадки *окно возможностей* для выработки общего подхода или хотя бы эффективной гармонизации существующих подходов достаточно быстро закроется. В результате мы рискуем оказаться в ситуации, когда множество государственных игроков участвуют в трансграничных кибероперациях по всему миру, руководствуясь лишь собственными либо узкогрупповыми представлениями о границах допустимого в этой сфере. Нетрудно предположить, что такая международно-правовая анархия, помноженная на трансграничный характер почти любой операции в киберпространстве, сможет очень быстро спровоцировать международные кризисы и даже вооруженные конфликты. Особенно опасным и угрожающим в этом свете выглядит тот факт, что реакция государств на недружественные действия в киберпространстве при отсутствии прозрачного и общепринятого международно-правового механизма разрешения разногласий может совсем необязательно ограничиваться киберпространством. На практике это будет означать растущий риск эскалации кризисов в киберпространстве до конфликтов с использованием кинетических вооружений.

На сегодняшний день ГПЭ ООН выглядит единственной достаточно широкой, авторитетной и компромиссной площадкой для того, чтобы попытаться все же приступить к выработке общепринятой консенсусной интерпретации Устава ООН и других ключевых норм международного права применительно к киберпространству и таким образом предотвратить описанный выше сценарий. Остается надеяться, что расширение мандата Группы в рамках ее пятого созыва в 2016 г. будет предусматривать работу над этой задачей. *Если не мы, то кто же?*

АНАТОЛИЙ СТРЕЛЬЦОВ: На мой взгляд, проблема стоит несколько шире, чем просто применение международного права в киберпространстве. Прежде все-

го надо ответить на вопрос, что особенного в применении международного права вообще? В отличие от права национального, это система норм и принципов, не просто регулирующих отношения между субъектами, в данном случае государствами, но система норм и принципов, которая применяется каждым государством самостоятельно. Правоприменителями выступают политические лидеры государств.

Если мы занимаемся борьбой с компьютерной преступностью в рамках национального законодательства, коллеги из Следственного комитета приносят в суд имеющиеся доказательства и говорят: «Вот заключение эксперта, напали такие-то личности, ущерб причинен такой-то». Когда речь идет о международном праве, картина меняется. Хрестоматийный пример — дело о проливе Корфу (Дело Международного Суда ООН 1947–49 гг.). Албания разрешила Югославии заминировать свои территориальные воды, а Англия решила продемонстрировать, что обладает достаточной силой, чтобы игнорировать нежелание Албании пропускать по этим водам международные корабли. В результате два британских эсминца наскочили на мины, 45 человек погибли и 42 получили ранения. Когда этот инцидент рассматривался в Международном Суде, основным доказательством служили свидетельства международных наблюдателей, по словам которых Албания вела за проливом непрерывное наблюдение. Без согласия Албании заминировать эти воды было нельзя. Никаких предупредительных табличек или других обозначений, которые говорили бы о том, что воды заминированы, не было. Таким образом, Албания создала ситуацию, в которой корабли, идущие в соответствии с нормами международного морского права, получили ущерб. По решению Международного Суда к Албании, соответственно, были применены санкции.

Есть общее мнение государств — членов ООН о том, что положения международного гуманитарного права применимы ко всем видам боевых действий. В связи с этим возникает вопрос: что такое боевые действия и средства, с помощью которых осуществляется насилие? В настоящее время в отношении Российской Федерации введены санкции. Насилие ли это? Да, экономическое. Это не вооруженное насилие, не военные действия. Разница в том, что военные действия осуществляются вооруженными силами с помощью оружия. Вспомним определение оружия — это устройство или механизм, предназначенный для поражения живой силы и техники. А что такое кибератака? Это злонамеренное использование информационных технологий, то есть процессов и методов обработки и передачи информации. Так могут ли методы обработки и передачи информации быть оружием?

К сожалению, практически любое слово, написанное в международных договорах, являющихся источником международного гуманитарного права, будучи рассмотрено в той плоскости, о которой мы говорим, становится достаточно проблемным, начиная с базовых определений. Что такое *театр военных действий* в киберпространстве, что такое *нейтральные государства*, где пролегают их границы, да и вообще, где находятся границы государств? Что такое международно-правовая ответственность государств? Хороший пример: в 2001 г. было решение Генассамблеи ООН по конвенции об ответственности государства за международно-противоправное деяние. Однако не надо забывать, что эта конвенция решением ГА ООН была принята к сведению и не более того, и с тех пор каждые три года представляется Генеральной Ассамблее и возвращается на доработку. Но при этом понятие *приписанной ответственности* гуляет по юридической литературе. Кто приписы-

вает ответственность? Каждое государство самостоятельно, потому что оно является правоприменителем в этой сфере.

Много споров сейчас ведется насчет того, что считать достаточным доказательством нападения в киберпространстве? Учитывая, что киберпространство — это пространство IP-адресов и доменных имен, и практически все, что можно отследить по бэктрекингу, всегда можно подделать, поскольку данные находятся в компетенции операторов, провайдеров, а каждый оператор находится в юрисдикции своего государства, то проблема достоверности доказательств кибернападения остается нерешенной.

Еще один важный вопрос — что такое оружие в киберпространстве. По сути, это использование информационных технологий для причинения ущерба, но в какой момент технология становится оружием? Для решения этой проблемы была предложена концепция *неявного оружия*. За основу был взят прецедент трагедии 11 сентября 2001 г. в США, в связи с которой Совет Безопасности ООН принял два решения, в которых согласился с тем, что средством вооруженного нападения не обязательно является оружие. Такая концепция не дает ответов на все вопросы, поставленные выше, но помогает классифицировать злонамеренное использование информационных технологий как разновидность вооруженной атаки или вооруженного нападения. Самый простой случай — хакерская атака. Простой, потому что возможности хакеров ограничены: бюджетом, количеством людей, которые могут быть привлечены к работе, и, следовательно, результаты, которых можно достичь с помощью злонамеренного применения технологий, тоже ограничены. Самым опасным субъектом враждебного использования информационных технологий является государство. Ведь таких возможностей и ресурсов, какие есть у государств, нет больше ни у кого. С этой точки зрения для нас небезразлично, кто осуществляет атаку. Ведь одно государство может сымитировать атаку с территории другого, чтобы возник конфликт, и совершенно непонятно, как классифицировать эти ситуации.

Применимость международного права имеет два аспекта. Первый — возможность правоприменителя использовать существующие нормы, чтобы регулировать свое поведение или реагировать на использование информационных технологий в качестве оружия. Второй — единообразное понимание ситуации, в которой осуществляется правоприменение. В Уставе ООН есть положения, касающиеся применения силы, но до сих пор нет ответа, могут ли информационные технологии рассматриваться в качестве силы. Я считаю, что в ряде случаев это возможно, например в тех случаях, когда речь идет о *неявном оружии*. Но отмечу, что *сила* в Уставе ООН рассматривается как вооруженная сила, а экономическая сила как сила уже не рассматривается. Получается, что, если использовать эту концепцию, дорабатывать Устав ООН и другие источники международного права нужно будет по минимуму.

Значительно сложнее вопрос о применении международного гуманитарного права. Он был поднят, и Мария Станиславовна правильно отразила эти важные проблемы, но я хотел бы еще подчеркнуть вопрос о суверенитете. Все международные отношения строятся на понятии суверенитета, а оно привязано к территории. Можно говорить о суверенитете в воздушном пространстве. Государственная граница в этом случае — это некая воображаемая линия, которая уходит вертикально

вверх от географической границы, закрепленной на карте международными договорами. Договоры, которые определяют государственную границу, рассматриваются как источник международного права при разрешении спорных вопросов. Международное морское право определяет, как закрепляется граница территориального моря, на которое распространяется государственный суверенитет.

В области определения государственной границы киберпространства ничего подобного нет. Впрочем, не совсем так считают наши американские коллеги, которые полагают, что к данному случаю может быть применен подход, предложенный в *Таллинском руководстве.* Авторы Руководства предлагают привязывать объекты киберпространства к территории страны. Но для увязывания IP-адресов объектов киберпространства с национальной территорией необходимы данные, которые есть, насколько я знаю, только у Корпорации по управлению доменными именами и IP-адресами (ICANN). Эта организация присваивает адреса и ведет учет распределения адресного пространства, сотрудничая с несколькими другими аффилированными организациями. У ICANN есть реальная возможность осуществлять контроль, но это американская компания. Возникает вопрос, как остальные государства будут реализовывать свои суверенные права, которые им приписывают, приписывая также ответственность за то, что они не предотвратили злонамеренное использование информационных технологий со своей территории? Ведь на это государство может ответить: где моя ответственность, где я подписался под этим, где проходит граница?

Недавно мы совместно с коллегами из ICANN проводили научно-исследовательскую работу, изучали вопросы обеспечения безопасности функционирования Интернета, дискутировали с американскими коллегами о том, существуют ли политические риски того, что Интернет может быть использован для нарушения суверенных прав государств? Американцы согласились с тем, что такие риски существуют.

В 2003 и 2005 гг. проходили Всемирные встречи на высшем уровне по вопросам информационного общества, в ходе которых китайские коллеги предложили интернационализировать управление Интернетом. С тех пор прошло больше десяти лет, но мы до сих пор не можем договориться, зачем это делать и в чем должна заключаться суть интернационализации. На мой взгляд, единственная цель интернационализации Интернета состоит в том, чтобы предотвратить ограничение функционирования Интернета в одной стране по политическому решению руководства другой страны. Возможно, необходимо создать под эгидой Совета Безопасности ООН организацию, которая принимала бы такие решения на основании норм международного права вместо частной организации, находящейся под юрисдикцией того или иного государства. Для нас это важно. Мы не готовы делегировать это право США. У нас есть основания не доверять им, но оттого что мы не вполне доверяем американским коллегам, мы не перестаем быть членами международного сообщества. Поэтому проблему надо решать на многосторонней основе.

Возможно, было бы целесообразно создать международную организацию, которая бы занималась решением задач объективизации и атрибуции опасных для международной безопасности случаев злонамеренного использования информационных технологий. Если это делать в международном масштабе, а также выве-

сти операторов определенного уровня из-под национальной юрисдикции и отдать их под юрисдикцию международную, это поможет решить проблему. Пример такой организации — Международный орган по морскому дну, существующий в рамках международного морского права. Действительно, не видно, что делает государство на дне морском, но есть организация, которая пытается урегулировать возникающие в этой области проблемы.

Первым шагом, на мой взгляд, должна стать выработка международных правил поведения, хотя бы необязательных. В конце концов все принципы международного права до некоторой степени носят декларативный характер. В этом плане правила поведения в киберпространстве не будут сильно отличаться от остальных принципов. Группа правительственных экспертов ООН по международной информационной безопасности, которая закончила работу в 2015 г., уникальна потому, что впервые эксперты согласились с тем, что можно и нужно подумать над тем, что можно было бы положить в основу дальнейшего обсуждения регулирования поведения государств в киберпространстве.

Вторым шагом могло бы стать обсуждение того, как трактовать и отражать в международных договорах злонамеренное использование информационных технологий в киберпространстве против территориальной целостности и политической независимости других государств. Потому что наиболее действенным источником международного права является прежде всего международный договор.

АНДРЕЙ КОЗИК: Полагаю эту тему очень актуальной. Хочу отметить, что кроме нарастающей статистики применения кибервзаимодействия государств растет обсуждение проблемы в академических кругах.

Действительно, создано несколько площадок для межгосударственного диалога. Группа правительственных экспертов (далее — GGE), о которой уже шла речь, — одна из них. Однако GGE, в работе которой мне посчастливилось принимать участие, — это в меньшей степени юридический, скорее, политический форум. Любые решения, которые он принимает, хороши тем, что принимаются они на основе консенсуса. Но судить о применимости международного права на основании решений GGE я бы не стал. В лучшем случае, только лишь о политической составляющей вопроса. Что касается моего опыта работы в группе, то мне показалось, что наиболее настороженно, хотя и по различным основаниям, к применению международного права отнеслись делегации Китая и России. В работе группы и в итоговых документах чувствуется эта настороженность. Даже там, где применение международного права очевидно, — государства пытаются смягчить формулировки, опасаясь, видимо, быть связанными своей позицией в будущем.

Однако право — это не политика. Оно консервативно, и норма, разработанная 50 лет назад, во время отсутствия предмета обсуждения, вполне может применяться сегодня. Так, ничто не помешало Международному суду ООН в Консультативном заключении о правомерности использования ядерного оружия сослаться на оговорку Мартенса, ставшей юридической нормой задолго до изобретения ядерной бомбы. Поэтому все те общественные отношения, которые уже урегулированы международным правом, продолжают ему подчиняться — не важно, с приставкой они *кибер-* или нет. При этом, что действительно важно, следует иметь в виду, что появляются и принципиально новые общественные отношения, которые раньше правом либо не регулировались, либо применение к ним суще-

ствующих норм приводит к конфликту самих норм в системе. Например, сложным вопросом является то, что в современной компьютерной сети информация, проходя путь от одного компьютера к другому, проходит по территории многих государств. Это нетипичная для международного права ситуация. В такой ситуации несут ли ответственность государства, если знают, что это вредоносный код? Каков предел их ответственности? Если государство желает действовать добросовестно, какими действиями ограничивается его поведение? Должно ли оно в ущерб своим интересам предпринять что-либо и т. д.? Здесь также возникают вопросы правомерности прослушивания телефонов лидеров государств и вообще электронного шпионажа.

Поскольку для многих государств неукоснительное применение норм международного права является приоритетом, были запущены академические проекты, призванные оценить применимость международного права к конкретным правоотношениям. Самым успешным и известным таким проектом является Таллинское руководство, созданное под руководством американского профессора Шмита международной группой экспертов. В настоящее время готовится вторая версия документа. Я имею удовольствие быть экспертом рабочей группы. Могу сказать, что это чисто академическая работа. Все нормы принимаются группой консенсусом, что бывает непросто. Группа объединяет экспертов со всего мира — от Австралии и Канады до Беларуси и Таиланда. Итоговый документ планируется подготовить в 2016 г.

Почему у европейцев и американцев находятся ресурсы для организации таких крупных научных проектов? Дело в том, что здесь есть понятные цели. Во-первых, и об этом не надо забывать, это престиж страны или организации, которая такое исследование проводит и публикует. То же Таллинское руководство пишется таким образом, чтобы любой прочитавший практик смог его немедленно применить. Оно издается ведущим академическим издательством и, как следствие, попадает в ведущие библиотеки мира, в министерства обороны, иностранных дел и другие профильные органы. Во-вторых, это влияние на практику государств. У нас масса примеров, когда академическая или общественная работа привела к созданию серьезных международных документов и изменению практики — вспомнить ту же Оттавскую конвенцию о запрещении противопехотных мин и проблематику химического оружия.

Для таких стран, как Россия, и таких организаций, как ОДКБ, на мой взгляд, создание подобных проектов жизненно важно. К сожалению, у нас традиционно мало внимания уделяется академической составляющей, а постсоветская наука международного права по прежнему обособлена от всего мира. Боюсь, что пока мы, вместо того чтобы создавать свои проекты и приглашать в них иностранных специалистов, будем критиковать чужие, так все и останется. Не думаю, что это конструктивно. Поэтому, на мой взгляд, долгосрочным устойчивым способом развития является создание и поддержание международных научных проектов. Это принесет ощутимую пользу и доктрине международного права, и нашим странам.