Confidential

RUSSIA

The circulation of this report has been strictly limited to the members of the *Trialogue* Club International and of the Centre russe d'études politiques.

This issue is for your personal use only.

Published monthly in Russian and in English by *Trialogue Company Ltd.*

Issue № 10 (226), vol.14. October 2015

6 ноября 2015 г.

Олег Демидов сообщает из Москвы:

ОТВЕТСТВЕННОСТЬ ГОСУДАРСТВ ЗА ПРОТИВОПРАВНЫЕ ДЕЙСТВИЯ В КИБЕРПРОСТРАНСТВЕ: ДИСКУССИЯ В МИРЕ И РОССИИ

АННОТАЦИЯ

По мнению консультанта ПИР-Центра Олега Демидова, к 2015 г. в мире окончательно утвердился дискурс о необходимости выработки для государств обязывающих норм поведения в киберпространстве. В статье анализируется вклад в этот процесс Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ ООН), возникшей по российской инициативе. Рассматриваются ключевые для данной дискуссии проблемы атрибуции кибератак и возможных ответных мер на них в русле взглядов ведущих российских и международных экспертов.

Автор предостерегает, что в результате нескоординированной деятельности различных государств и региональных альянсов по интерпретации международного права применительно к киберпространству мир рискует оказаться в ситуации международно-правовой анархии в данной сфере, способной спровоцировать международные кризисы и даже вооруженные конфликты. При этом наиболее подходящей площадкой для выработки общепринятой консенсусной интерпретации Устава ООН и других ключевых норм международного права применительно к киберпространству автору представляется ГПЭ ООН.

ГПЭ: ПЕРВЫЕ ШАГИ НАВСТРЕЧУ РЕЖИМУ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ В КИБЕРПРОСТРАНСТВЕ

22 июля 2015 г. был опубликован новый доклад *Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ ООН)*. Он стал плодом годовой работы уже четвертого по счету созыва Группы, действующей с 2001 г., и содержит в себе свод политических норм, предлагаемых государствам-членам ООН в качестве первого шага к режиму ответственного поведения в киберпространстве.

Хотя сама ГПЭ имеет на Западе неоднозначный имидж детища российской инициативы, служащего прежде всего интересам Москвы, ее деятельность привлекает все большее внимание в мире - в частности, став ключевым предметом обсуждения на 4-ой Глобальной конференции по киберпространству, прошедшей в апреле 2015 г. в Гааге, Нидерланды.

Проявившийся в Гааге разворот западных дипломатов и экспертного сообщества, включая частный и правительственный сектор, навстречу ГПЭ 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 не нуждается в обязывающих нормах.*
- ***Во-вторых**, стало очевидно, что несмотря на хронические противоречия по ключевым вопросам между членами ГПЭ (прежде всего, между РФ и США), работа Группы все же плодотворна и по большому счету безальтернативна, ибо ООН – единственная глобальная площадка, на которой имеет смысл договариваться об общих правилах для трансграничного киберпространства.*

Росту внимания к работе ГПЭ послужило и то, что с третьего созыва в повестку Группы была включена фундаментальная задача – адаптация к киберпространству существующих норм международного права, включая Устав ООН. В докладе ГПЭ 2013 г. было впервые заявлено, что Устав ООН применим к киберпространству, а в Докладе 2015 г. ГПЭ удалось согласовать ряд ключевых посылок о применимости международного права к киберпространству:

- признание суверенитета государств над ИКТ-инфраструктурой в пределах их территории;
- необходимость соблюдения в киберпространстве таких международно-правовых принципов, как 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;
- 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, эти посылки являются, конечно, лишь общими отправными точками, за которыми необходимо решение более серьезных прикладных вопросов. В числе таковых – проблема атрибуции кибератак и согласования ответных мер на кибероперации, признанные актами применения силы (включая критерии такого признания).

ПРОБЛЕМА АТРИБУЦИИ И ОТВЕТНЫХ МЕР: МЕЖДУНАРОДНАЯ И РОССИЙСКАЯ ДИСКУССИЯ

Очевидно, что атрибуция кибератак с вовлечением государств имеет практический смысл только в том случае, когда определены возможные ответные меры в отношении актора противоправных действий в киберпространстве.

Для конкретного примера можно обратиться к хорошо известной ситуации с вирусом *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 и организации трансграничного расследования удалось бы добыть технические свидетельства причастности АНБ и Моссада к операции по кибersаботажу иранских атомных объектов. 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?

Характерно, что ведущие эксперты и дипломаты России и стран НАТО не могут дать ответа на этот вопрос. Это будет невозможным до тех пор, пока не будет прояснена интерпретация ключевых понятий международного права применительно к киберпространству. Ведущие российские эксперты в этой области **А.А. Крутских и А.А. Стрельцов** в статье 2014 г. в журнале *Международная жизнь* и авторы *Таллиннского руководства по применению международного права в условиях конфликта в киберпространстве* CCDCOE (Cooperative Cyber Defense Center of Excellence, Центр совместной киберзащиты) **НАТО** приводят практически идентичный перечень этих понятий, среди которых три наиболее важных –

- угроза силой или применение силы (Статья 2(4) Устава ООН);
- акт агрессии (Статья 39 Устава ООН);
- вооруженное нападение (Статья 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 сейчас неизвестен именно в силу отсутствия общепринятой интерпретации Устава ООН для киберпространства.

Среди перечисленных терминов из Устава ООН наибольшая ясность присуща понятию агрессии, определению которой посвящена отдельная одноименная **резолюция ГА ООН №3314** от 4 декабря 1974 г. В ней приводится перечень из семи видов действий, подпадающих под понятие агрессии, с уточнением, что список этот 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 был проведен в недавней работе коллектива авторов Министерства обороны РФ. При этом **военные эксперты МО РФ** продвигают идею не обновления текста резолюции, а его адаптированное прочтение, которое охватывало бы операции в киберпространстве, потенциально подпадающие под понятие агрессии. В частности, ими предложено 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). К действиям же хакерских групп-посредников предложено применять пункт g) (засылка государством или от имени государства вооруженных банд, групп, иррегулярных сил или наемников, осуществляющих применение вооруженной силы).

Однако эксперты Минобороны признают ключевой недостаток Резолюции ГА ООН – отсутствие у нее обязательной силы. 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* из Резолюции №3314 ГА ООН. Но для завершения процесса необходимо соответствующее решение на следующей обзорной конференции по Римскому Статуту МУС, запланированной на январь 2017 г. (хотя принятие решения может

быть отложено и на более дальнюю перспективу). До этого крайне желательно развить международную дискуссию об адаптации текста Резолюции №3314 (и, параллельно, понятия *преступление агрессии* в Римском Статуте МУС) к кибероперациям. Подходящей площадкой для такой дискуссии видится как раз ГПЭ ООН, следующий, пятый созыв которой ожидается в 2016 г.

ПОТЕНЦИАЛЬНЫЕ ПЕРСПЕКТИВЫ И РИСКИ ДЛЯ РОССИИ И МИРОВОГО СООБЩЕСТВА

Хотя участники ГПЭ, включая российских дипломатов, неоднократно подчеркивали, что мандат Группы не включает в себя глубокую ревизию норм международного права с целью их адаптации к киберпространству, логика подсказывает, что полностью скинуть с себя эту функцию Группе не удастся. Чем дольше ГПЭ будет избегать ее, тем больше шансов на то, что 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.

- Так, в свежем (от июня 2015 г.) издании *Руководства по праву войны* Министерства обороны США (*DoD Law of War Manual*) четко прописаны критерии и условия, при которых кибероперация квалифицируется как незаконное применение силы по смыслу Статьи 2(4) Устава ООН. 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.

- Одновременно, выводы, полученные в ходе работы над *Таллиннским 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 Углубленой доктрины кибероборонны Альянса. По его итогам было принято политическое решение о том, что право членов НАТО на коллективную оборону, заложенное в Статье 5 Вашингтонского договора, распространяется и те случаи, когда страна-член НАТО становится жертвой нападения в киберпространстве. Отныне кибератака на члена НАТО, повлекшая гибель людей или масштабное разрушение инфраструктуры и, с точки зрения 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 в каждом конкретном случае.

Потенциальные риски такого подхода хорошо иллюстрируются примером 2007 г., когда Эстония, ставшая жертвой мощной волны кибератак в разгар т.н. «кризиса Бронзового солдата» запросила руководство НАТО относительно возможности применения Статьи 5. При этом в качестве агрессора рассматривалась Россия, которую Эстония обвинила в организации и осуществлении кибератак, несмотря на отсутствие надежных доказательств. Повторись такая ситуация сегодня, с учетом новой доктрины кибероборонны НАТО речь могла бы идти о потенциальной эскалации кризиса между Россией и НАТО.

Для международного сообщества риск разноскоростной, нескоординированной деятельности различных государств и региональных альянсов по 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 мир рискует оказаться в ситуации, когда множество государственных игроков будут участвовать в трансграничных кибероперациях по всему миру, руководствуясь лишь своими 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. Ведь реакция государств на недружественные действия в киберпространстве при отсутствии прозрачного и общепринятого международно-правового механизма разрешения разногласий может не ограничиваться киберпространством.

В этом смысле выработка ГПЭ 11 «добровольных и необязательных норм, правил или принципов ответственного поведения государств», даже в качестве общих и сугубо добровольных предложений международному сообществу, стала значительным прогрессом а контексте развития диалога об ответственном поведении государств в киберпространстве. На сегодняшний день ГПЭ ООН выглядит единственной достаточно широкой, авторитетной и компромиссной площадкой для того, чтобы попытаться приступить к выработке общепринятой консенсусной интерпретации Устава ООН и других ключевых норм международного права применительно к киберпространству и тем самым предотвратить описанный выше сценарий.

Автор материала: Олег Демидов, консультант ПИР-Центра.

Редактор: Юлия Фетисова

Москва-Женева, Октябрь 2015 г.

Выдержки из документа «Международный Клуб Триалог. Условия и правила членства».

3. Права членов Клуба

3.1. Индивидуальные члены Клуба имеют право:
3.1.3. Получать 1 экземпляр бюллетеня эксклюзивной аналитики Russia Confidential по электронной почте, на выбранном языке (русском или английском). По правилам Клуба, передача бюллетеня третьим лицам не допускается.
[…]
3.2. Корпоративные члены Клуба имеют право:
3.2.3. Получать 2 экземпляра бюллетеня эксклюзивной аналитики Russia Confidential по электронной почте, на выбранном языке (русском или английском) либо на обоих языках одновременно, передавать этот бюллетень другим представителям корпоративного члена Клуба. По правилам Клуба, передача бюллетеня третьим лицам, не являющимся членами Клуба, не допускается.
[…]

4. Обязанности членов Клуба

4.1. Все срочные члены Клуба обязаны:
4.1.6. Не передавать полученные материалы бюллетеня Russia Confidential, а также пароли доступа на сайт Клуба физическим и юридическим лицам, не являющимся членами Клуба.
[…]

6. Russia Confidential

6.1. Бюллетень эксклюзивной аналитики Russia Confidential выпускается ООО «Триалог» исключительно для личного пользования членов Клуба.
6.2. Бюллетень содержит сжатую эксклюзивную аналитику по вопросам международной безопасности, внешней и внутренней политики России и государств СНГ, подготовленную ведущими экспертами специально для Russia Confidential.
6.3. В течение не менее 30 дней со дня выхода материалы бюллетеня являются конфиденциальными и не могут цитироваться и передаваться лицам, не являющимся членами Клуба.
6.4. По прошествии не менее чем 30 дней ООО «Триалог» может снять эксклюзивный и конфиденциальный статус с материала, после чего в этих случаях он может быть опубликован в других изданиях и может быть использован для цитирования членами Клуба.
6.5. Бюллетень распространяется по электронным адресам членов Клуба 1 раз в месяц по русском или английском языке, по выбору члена Клуба.
6.6. По запросу члена Клуба, он может также получить бумажную версию бюллетеня на выбранном им языке.

Уважаемые члены Международного клуба Триалог,

продолжается сезон-2015 работы Клуба, и мы рады **пригласить Вас продлить членство в Международном клубе *Триалог* на 2016 год или на 2016 - 2017 годы**, если Вы еще не сделали этого.

В 2016 г. члены Клуба продолжат получать от нас эксклюзивную информацию по вопросам, связанным с приоритетами внешней политики Российской Федерации, а также современными вызовами и угрозами международной безопасности. На 2016 г. запланировано проведение **5 заседаний Международного клуба *Триалог***, 4 из которых пройдут в Москве, а 1 за рубежом. Члены клуба получат 4 номера ежеквартального журнала *Индекс Безопасности в электронном виде и 2 номера в печатном* (в 2016 г. только на русском языке), **12 номеров** бюллетеня эксклюзивной аналитики *Russia Confidential* (на русском или английском языке), наши электронные информационные и аналитические рассылки.

Как и прежде, специалисты Международного клуба *Триалог* и партнерской организации ПИР-Центра открыты к обмену мнениями по ключевым международным проблемам.

С 2016 г. размер ежегодного взноса за членство в Клубе *Триалог* составляет:

Период	Индивидуальное членство	Корпоративное членство
01.01.16. – 31.12.16. (1 год)	50 000 руб.	80 000 руб.
01.01.16. – 31.12.17. (2 года)	90 000 руб.	140 000 руб.

Напоминаем Вам, что в рамках **корпоративного** членства действует **схема «1+1»**, когда в работе Клуба участвуют **два представителя** одной организации.

Обращаем Ваше внимание, что при оплате членских взносов не позднее 30 ноября года, предшествующего году членства, за который проводится оплата, предоставляется скидка в размере 10% от суммы взноса.

По всем вопросам, связанным с членством в Международном клубе *Триалог*, следует обращаться по электронной почте secretary@trialogue-club.ru или по тел.: +7 (985) 764-98-96.

С уважением,

Председатель,
Международный клуб *Триалог* **Д.В. Поликанов**