Шесть коротких замечаний относительно Таллиннского руководства CCD COE

Олег Демидов, координатор программы «Международная информационная безопасность и глобальное управление интернетом», ПИР-Центр

19 марта с.г. был опубликован окончательный вариант Таллиннского руководства по вопросам применения международного права к вопросам киберконфликтов – документ, подготовленный группой экспертов Центра совместной киберобороны НАТО в Таллинне. Несмотря на то, что руководство пока не имеет никакого официально статуса, и более того, неизвестно, получит ли оно подобный статус в будущем, его появление вызвало бурный интерес как в самих странах НАТО, так и в России. Почти 300-страничный документ привлек к себе всеобщее внимание прежде всего в силу отдельных положений, вызвавших дискуссии в связи со своим новаторским для международного права и «проактивным» характером.

Положения Таллиннского руководства при определенных условиях санкционируют применение неограниченно широкого спектра кинетического оружия против источника киберугрозы, силовые действия в отношении гражданских хактивистов (путем приравнивая их к комбатантам), а также ответные кибероперации, направленные против чужой критической инфраструктуры – включая атомные станции и дамбы плотин. Наличие подобных положений, основанных на не всегда единогласном экспертном консенсусе авторов руководства, дало основание ряду специалистов и экспертов утверждать, что документ задает горизонт возможностей государствам для осуществления кибероперaций – в том числе с далекоидущими последствиями в материальном и международно-политическом плане. Иными словами, речь идет якобы о легитимации киберконфликтов как формы поведения государств и действующих от лица посредников (англ. *proxy actors*) на мировой арене.

В частности, подобные соображения высказывались представителями российских Минобороны и Министерства иностранных дел РФ, а также Генштаба ВС РФ и некоторыми авторитетными отечественными экспертами в вопросах кибероборонны в ходе круглого стола «*Новые рекомендации НАТО по войне в киберпространстве: приглашение к диалогу или провокация? Международные оценки и взгляд из России*», который прошел 31 мая 2013 г. в Москве. Также участники дискуссии охарактеризовали документ как «катехизис по ведению информационных войн». Любопытно, что такая позиция в отношении Таллиннского руководства вызывает

довольно острый интерес и ряд вопросов среди зарубежных - и прежде всего западноевропейских экспертов. Мое выступление по Таллиннскому руководству на сессии *Европейского диалога по управлению интернетом (EuroDIG 2013)* в июне 2013 г. спровоцировало дискуссию о российской позиции по документу, а также о том, какие существуют основания для интерпретации норм руководства в качестве инструкций для провоцирования и ведения киберконфликтов.

Не претендуя на подробный анализ и окончательный характер оценок, хотелось бы сформулировать ряд кратких комментариев по ключевым вопросам, которые ставит этот документ перед Россией и международным сообществом.

1. Таллиннское руководство, прежде всего, представляет собой одну из первых системных попыток заполнить международно-правовой вакуум в части формулирования правил поведения государств как субъектов и прямых участников конфликтов в киберпространстве. С этой точки зрения, речь идет о важном заделе на будущее, в отсутствие которого возможный крупный киберконфликт может столкнуть международную систему в ситуацию дезориентации, неадекватной и непропорциональной реакции на враждебные действия в киберпространстве. Что безусловно чревато неуправляемым перетеканием конфликта из киберпространства в плоскость реальных вооруженных столкновений.

Не менее важно, что Таллиннское руководство в этом смысле не является попыткой произвольного нормотворчества и однозначно опирается на утвердившуюся и признаваемую в глобальном масштабе базу международного гуманитарного права (МГП) и права вооруженных конфликтов. Таким образом, сама идея, лежащая в основе документа, представляет собой шаг в правильном и нужном направлении. Вопросы скорее кроются в особенностях избранного подхода, а также международно-политической конъюнктуре, влияющей на интерпретацию выводов и положений документа.

2. Вопреки часто звучащему мнению, Таллиннское руководство не может рассматриваться в качестве естественного антагониста российского подхода, во главе которого лежит подчинение поведения государств в информационном пространстве специальному своду универсальных и юридически обязывающих норм. Разница между двумя подходами заключается прежде всего в том, что они рассматриваются через призму разных установок и задач. Если Россия и ее союзники видят свою миссию в том, чтобы не допустить межгосударственных киберконфликтов и вывести такие явления за рамки приемлемых действий на международной арене, то Таллиннское руководство – документ, не несущий такой задачи и отвечающий скорее на вопрос «Что делать, если гром все же грянул?».

Таким образом, российские дипломаты и эксперты Центра совместной кибероборонв Таллинне работают на разную постановку задачи, но при этом их подходы не являются взаимоисключающими. Женевские и Гаагские конвенции, от которых отталкиваются авторы Таллиннского документа, возникли в свое время именно потому, что войны между государствами тогда были частым и неизбежным

явлением, и в ситуации, когда их нельзя было прекратить как таковые, государства выработали *правила* их ведения с тем, чтобы ограничить жертвы мирного населения и ущерб от военных конфликтов, гуманизировать войну. Был бы возможен полный запрет агрессивной войны в 1945 г. без принятия ранее Женевских и Гаагских конвенций – большой вопрос.

3. В этой связи важно, что положения концепции Конвенции об обеспечении международной информационной безопасности (концепция Конвенции о МИБ), - одной из ключевых составляющих российского подхода – содержат прямую ссылку на подход, лежащий в основе Таллиннского документа. Речь идет о Статье 7, пункте 2, согласно которому «*в случае любого международного конфликта право государств-участников, находящихся в конфликте, выбирать методы или средства ведения «информационной войны» ограничено* ***применимыми нормами международного гуманитарного права***».

Таллиннское руководство и есть подробная инструкция на этот самый случай, и может быть, руководству России и НАТО скорее следует задуматься над тем, как постепенно выработать возможность взаимного дополнения и усиления двух подходов – ведь друг без друга оба они грешат неполнотой и однобокостью. Таллиннское руководство, не будучи подкреплено какими-либо международными нормами, сдерживающими государства от кибервойн, действительно может способствовать легитимизации киберконфликтов, врастанию их в систему международных отношений в XXI веке в качестве допустимого средства решения внешних задач и обеспечения национальных интересов. Нужен балансир в виде международно-правовых ограничений, в духе которых действует и Россия. Однако в условиях мер верификации, нерешенной проблемы атрибуции и невероятно низкого технологического и ресурсного порога создания и применения кибероружия российские инициативы пока напоминают попытку удержать в руках воду – и потому лишь выиграют, если вберут в себя корпус норм и правил, дающих ответ на вопрос «Что делать, если запрет все же нарушен?».

Однако надо отдавать отчет в том, что сближение и гармонизация двух подходов – задача на отдаленную перспективу, полагать иначе в условиях дефицита взаимного доверия по вопросам киберпространства между Россией и НАТО, Россией и США было бы наивно. А вот заняться наработкой такого капитала доверия, начиная с обмена технической информацией – достойная и крайне своевременная задача. К тому же она как раз начала решаться на двустороннем уровне с подписанием совместного заявления президентов России и США о сотрудничестве в укреплении доверия в области ИКТ в рамках встречи президентов двух стран на полях саммита «Большой восьмерки» в Северной Ирландии 17 июня с.г.

4. Отдельный интерес вызывает позиция США по отношению к Таллиннскому руководству. Мнение, согласно которому документ прямо отражает позицию США как ведущей кибердержавы, чью стратегию определяет принцип проактивных действий (в том числе силовых) и глобальное доминирование в киберпространстве – плохо соотносится с некоторыми положениями руководства. Например, с

параграфом о том, что «государства несут прямую ответственность в соответствии с международным правом за любые действия отдельных лиц или групп, которые действуют по его непосредственному указанию». Этот принцип в случае его утверждения в качестве общепризнанной нормы прямо противоречит усилиям Киберкомандования США по привлечению американских хакеров к решению задач национальной безопасности в киберпространстве – включая кибероборону.

5. В то же время, многие положения Таллиннского руководства – в частности – норма о допустимости использования военного ответа в киберпространстве против гражданских хактивистов, а также норма о возможности использования кинетических средств против кибератак – действительно отвечает интересам США, так как позволяет, оставаясь в рамках международного права, противодействовать группам и лицам, чью связь с госструктурами выявить невозможно – например, с китайскими хакерами и кибершпионами, которые сегодня позиционируются в качестве главной угрозы кибербезопасности США.

6. Основное опасение, которое возникает, если рассматривать Таллиннское руководство как инструкцию по выработке стратегии поведения в условиях киберконфликтов для НАТО, международного сообщества вообще и конкретно США, связано с наличием весьма обширного пространства для интерпретаций международного права, которое создает заложенный в документе подход. Таллиннское руководство – и это принципиальный момент – является не универсальной адаптацией норм международного гуманитарного права, а лишь их *прочтением* группой экспертов. Поскольку речь идет о специфичной реальности киберпространства, положения Таллиннского руководства оказываются довольно далеки от исходных норм МГП и права вооруженных конфликтов, а само их прочтение оказывается сильно подверженным интерпретации. Нет никакой гарантии, что в скором будущем США, осуществляя уже самостоятельное прочтение международных норм по тому же принципу, аналогично таллиннским экспертам определят границу для использования военной силы в ответ на кибератаку, порог перехода гражданских хактивистов в статус комбатантов и легитимных целей на поле боя – и так далее.

В заключение следует подчеркнуть - пожалуй, наиболее принципиальный вопрос применительно к Таллиннскому руководству состоит именно в значительной степени свободы прочтения существующих норм МГП, заложенной в самом его подходе. Подобная *свобода интерпретации* потенциально оставляет для каждого отдельно взятого государства слишком большой люфт, чтобы сделать его поведение в киберпространстве предсказуемым для остальных государств. Отсюда возникает следующий вопрос – что станет следующим шагом после Таллиннского руководства и насколько четкий и единообразный свод правил будет создан в итоге – и будет ли? Однако даже если страны НАТО пройдут весь путь и разработают собственный единогласно признаваемый и единообразно интерпретируемый вариант адаптации международного гуманитарного права для киберпространства, последуют ли ему на национальном уровне США? Поймут ли его Россия, Китай, Индия и еще 150 стран?

И здесь мы возвращаемся к тому, о чем с 1998 г. говорят российские дипломаты – о всеобщей «договоренности» относительно универсальных правил поведения в киберпространстве – либо, по крайней мере, глобальной договоренности о том, как формировать и понимать такие правила. Обойтись без этого будет нелегко. В этом смысле с российской позицией трудно спорить, так как без универсального признания и единого понимания любое развитие Таллиннского руководства будет иметь сильно заниженную ценность. Или действительно препятствовать снижению конфликтного потенциала в киберпространстве из-за разницы в понимании существующих международно-правовых норм, давая дальнейшую пищу критикам документа.

***

Принимая во внимание фундаментальную значимость проблем, затрагиваемых Таллиннским руководством, ПИР-Центр планирует осуществлять их дальнейшее исследование в рамках своей программы «*Международная информационная безопасность и глобальное управление интернетом*». Мы будем рады услышать комментарии и соображения читателей бюллетеня относительно Таллиннского руководства и в целом регулирования поведения государств в киберпространстве и информационном пространстве. Данные вопросы будет рад обсудить с вами координатор программы ПИР-Центра, выпускающий редактор бюллетеня «Пульс кибермира» Олег Демидов (demidov@pircenter.org).