УДК 355.01

© Гриняев С.Н.
Grinyaev S.

«ТАЛЛИННСКОЕ РУКОВОДСТВО ПО ПРИМЕНЕНИЮ ЮРИДИЧЕСКИХ НОРМ МЕЖДУНАРОДНОГО ПРАВА К ВОЕННЫМ ДЕЙСТВИЯМ В КИБЕРПРОСТРАНСТВЕ» В ОЦЕНКАХ ЗАПАДНЫХ ЭКСПЕРТОВ

"TALLINN GUIDANCE ON THE APPLICATION OF LEGAL NORMS OF INTERNATIONAL LAW FOR MILITARY ACTION IN CYBERSPACE "IN THE ESTIMATES OF WESTERN EXPERTS

Аннотация. *В статье рассматривается документ, получивший название «Таллиннское руководство по применению юридических норм международного права к военным действиям в киберпространстве», а также его оценки со стороны американских и европейских экспертов. Показано единство позиций и различие во взглядах на документ со стороны экспертного сообщества.*

Annotation. *In the article the paper, titled "Tallinn guidance on the application of legal norms of international law for military action in cyberspace", as well as its assessment by the U.S. and European experts. Displaying unity of positions and differences in views on the document from the expert community.*

Ключевые слова. *«Таллиннское руководство», юридическое право, информационное право, информационные войны, правила и нормы ведения войны.*

Key words. *«Tallinn Guide», a legal right, the right to information, information warfare, the rules and the rules of war.*

Документ, известный как «Таллиннское руководство по применению юридических норм международного права к военным действиям в киберпространстве»[1] (далее Руководство), достаточно высоко оценивается как американскими, так и европейскими экспертами, хотя и вызывает неоднозначные суждения по некоторым аспектам. Эксперты сходятся во мнении, что Руководство является первым документом подобного рода и закладывает основы юридического обеспечения применения средств ведения информационно-технического противоборства в компьютерных сетях.

Основной вывод, заключается в том, что, согласно существующим взглядам, *основные принципы международного права применимы к действиям в киберпространстве.* В контексте вооруженного столкновения законы и правила вооруженной борьбы применимы и для использования средств информационной борьбы.

Также эксперты считают, что информационное пространство ничем не отличается от иных сфер противоборства и не требует особых подходов к его юридическому обеспечению.

Вместе с тем, ряд понятий и норм международного права все же требует уточнений для действий в киберпространстве. В частности, до конца нерешенным остается вопрос о трактовке понятия "агрессия" в отношении к информационным операциям. Также окончательно не разработаны понятия суверенитета, нейтралитета и пропорционального использования силы.

Ключевым тезисом Руководства является тезис о том, что *применение средств информационного воздействия есть применение силы, соответствующее таковому понятию в Уставе ООН и общепринятом международном праве. Также и запрет на использование силы трактуется в соответствии с Уставом ООН.*

В этом контексте эксперты указывают на возможное смешение понятий «использование силы» и «вооруженного нападения». В частности указывается, что Устав ООН дает право государству ответить на нападение лю-

[1]«Tallinn Manual on the International Law Applicable to Cyber Warfare», Michael N. Schmitt (Editor) , http://www.amazon.ca/Tallinn-Manual-International-Applicable-Warfare/dp/1107024439

Гриняев Сергей Николаевич – доктор технических наук, старший научный сотрудник, генеральный директор, АНО «Центр стратегических оценок и прогнозов», тел.+7 (916) 633-75-23.

Grinyaev Sergei – PhD, senior research fellow, director general, NGO "Center for strategic studies and forecasts", tel. +7 (916) 633-75-23.

быми доступными средствами (т.е. традиционными или информационными). В то время как использование запрета на применение силы относится только к действиям государств (или государственным структурам), право на самооборону охватывает также и действия, предпринятые негосударственными акторами. Не проработанным остается вопрос относительно того, когда такие операции составляют «использование силы», причем такой, что они запрещены Уставом ООН (т.е. не относятся к самообороне и не реализуются по мандату Совета Безопасности ООН). Здесь мнение европейских и американских экспертов расходится.

Для американских экспертов физические последствия информационной операции есть ключ к трактовке правомерности применения силы. Действия в киберпространстве, которые непосредственно приводят к ранению или гибели людей или существенным разрушениям инфраструктуры *могут* рассматриваться как использование силы.

Европейские эксперты считают, что информационная операция есть «использование силы», когда ее масштаб и последствия сопоставимы с применением конвенционального оружия, т.е. в случае, если применение средств информационной борьбы ведет к ранению или гибели людей. Такие действия *однозначно* рассматриваются как применение силы. Т.е. европейская позиция в этом вопросе более жесткая и четкая, нежели американская, допускающая различное толкование.

Существует проблема четкой идентификации последствий применения информационного оружия и их сравнения с результатами использования традиционных средств поражения. Так, существуют информационные операции, которые не приводят к явным последствиям в физическом пространстве. В этом случае эксперты полагают, что такие действия не могут рассматриваться как «применение силы» и, следовательно, в этом случае не могут быть вовлечены вооруженные силы. Таким образом, вопрос о том, какие действия считать «применением силы», особенно для случаев, в которых не проявлены эффекты в физическом пространстве, остается открытым. Для решения указанной задачи предложен вероятностный подход, по которому государство с определенной вероятностью будет считать конкретные действия в информационном пространстве «применением силы». Этот подход базируется на оценке ряда факторов. Из них наиболее существенным является фактор "серьезности" воздействия. Именно согласно этому фактору, информационную операцию в киберпространстве, которая приводит к повреждению/разрушению инфраструктуры, ранению или гибели людей, с большей вероятностью будут считать «применением силы» независимо от других факторов.

Согласно мнению экспертов, государство, которое является целью информационной атаки, оцененной как вооруженное нападение, может реализовать право на самооборону. И европейские, и американские эксперты соглашаются, что информационные операции, в результате которых гибнут или страдают люди или наносится серьезный материальный ущерб объектам инфраструктуры, являются вооруженным нападением на страну. В этом случае ответные действия могут быть предприняты как с использованием традиционного, так и информационного оружия при соблюдении принципов целесообразности и пропорциональности.

Важным является вопрос о многократных информационных атаках на объекты инфраструктуры, каждая из которых не является в отдельности вооруженным нападением. Вопрос, могут ли «булавочные уколы» быть объединены в единую цепь событий, которая будет истолкована как вооруженное нападение, остается неразрешенным. Вместе с тем, эксперты согласились, что в соответствии с принципом «накопления последствий», такие разрозненные, но целенаправленные действия, могут быть расценены как вооруженное нападение. Однако при этом источник атак должен быть один, для всех атак должны быть сходные цели и для каждой из атак должен быть превышен определенный порог последствий.

Американские эксперты поддерживают так называемую «превентивную оборону», т.е. заблаговременное применение силы перед лицом неизбежного нападения. Большинство европейских экспертов соглашается с тезисом, что международное право разрешает «упреждающую самооборону». Соответственно в Руководстве отмечено, что право применить силу для самообороны возникает, если нападение с применением средств информационной войны уже происходит или неизбежно.

Вместе с тем, *европейские эксперты категорически отклонили понятие о «профилактической самообороне»* – действий, предпринимаемых в ответ на возможное нападение, когда противник уже обладает возможностью провести такое нападение, но не принял политического решения.

Остается нерешенным вопрос об адекватном ответе, когда в качестве агрессора выступает негосударственный актор. Вопрос о том, могут ли действия, предпринимаемые таким актором расцениваться как вооруженное нападение и провоцировать ответное применение силы, окончательно не решен.

Эксперты указывают, что в соответствии с нормами действующего права необходимо строгое различие между гражданским населением и личным составом воюющих армий, а также гражданскими и военными целями. Соответственно применение военной силы должно быть направлено только против военных целей. Справедливость этого тезиса не оспаривается большинством экспертов.

В оценке применимости этой нормы важным остается вопрос об идентификации понятия «военная цель» для информационного пространства.

Отмечено требование международного гуманитарного права о необходимости для нападающего различать военные и гражданские объекты: нападения допустимы только против военных целей. *Военными считаются те объекты, которые по их характеру, местоположению, цели создания или использования оказывают вклад в военные действия и чье полное или частичное разрушение, захват или нейтрализация в сложившейся ситуации предполагает определенное военное преимущество. Трактовка этого определения показывает следующее: компьютерная сеть военного назначения и гражданский сервер, используемый для передачи военных данных (среди прочих), являются военными целями.*

Позиция американских экспертов выходит за рамки этого определения. Прежде всего, они полагают, что *определение не должно ограничиваться только сугубо военными целями и целями, поддерживающими функционирование военной инфраструктуры, а должно также включать и цели, служащие для поддержания способности государства вести военные действия.* В частности, среди таких целей могут быть объекты нефтедобычи, если в стране-противнике прибыль от экспорта нефти служит для формирования военного бюджета, а также иные инфраструктурные объекты, используемые при формировании оборонного бюджета.

Также от экспертов потребовалось определить ущерб гражданским объектам, который расценивается как сопутствующий при оценке пропорциональности применения силы.

Соответственно, «сопутствующие разрушения» есть потери среди гражданского населения, повреждение или разрушение гражданской инфраструктуры во время информационной операции против установленной военной цели. Все остальные психологические, эмоциональные и иные последствия, такие как неудобство, раздражение, напряжение или страх, не могут рассматриваться в качестве сопутствующего ущерба. Кроме того, большинство экспертов согласилось, *что потеря данных не составляет сопутствующий ущерб, если такая потеря не вредит нормальному функционированию гражданского объекта.*

В контексте сопутствующих потерь, а также разделения военных и гражданских целей американскими экспертами широко обсуждается термин «инфраструктуры двойного использования» в киберпространстве (т.е. инфраструктуры, одновременно используемой военными и гражданскими потребителями). Несмотря на то, что идентификация целей двойного применения затруднена в информационном пространстве, отмечено, что *ее выведение из строя укладывается в понятие пропорционального применения силы.*

Важным аспектом рассматриваемой проблемы юридического обеспечения действий в информационном пространстве является понятие «национального суверенитета». Соответственно, государства, проводящие действия в киберпространстве, должны принять во внимание суверенитет других государств.

Эксперты сошлись во мнении, что государства могут осуществить любые действия в отношении любой инфраструктуры, расположенной на их суверенной территории. Территориальный суверенитет также предоставляет защиту инфраструктуре в соответствии с международным правом независимо от формы собственности.

В осуществлении целей обеспечения безопасности государство может закрыть доступ к Интернет. Важным является факт, что *инфраструктура, расположенная на территории государства, но при этом связанная с глобальной телекоммуникационной сетью, не может интерпретироваться как экстерриториальное образование и на этом основании лишенное суверенных прав государства на нее.*

Информационная операция нарушает государственный суверенитет, если физическое повреждение от ее проведения вызвано в инфраструктуре, расположенной на территории этого государства.

Эксперты отмечают, что две формы территориальной юрисдикции – субъективная и объективная являются особенно существенными при правовой оценке действий в информационном пространстве. Когда операция начата на территории того или иного государства, оно обладает субъективной юрисдикцией независимо от того, где проявляются эффекты от реализации этой операции. Объективная территориальная юрисдикция предоставляет государственную юрисдикцию по операциям, начатым вне территории государства, но оказывающим воздействие на объекты инфраструктуры на его территории.

Также подчеркивается, что из понятия суверенитета вытекают не только права, но и обязательства госу-

дарства. Так, государство не должно содействовать использованию инфраструктуры, расположенной на ее территории или под ее исключительным контролем, для действий, направленных против иных государств. Государство обязано принять все доступные меры для предотвращения информационного нападения со стороны криминальных и террористических групп, действующих с территории этого государства против иных государств.

Во время международного вооруженного столкновения указанные выше принципы используются для оценки нейтралитета того или иного государства и *в случае нарушения установленных правил государство может быть отнесено к одной из воюющих сторон.* Таким же образом государства несут ответственность за действия в информационном пространстве, предпринимаемые акторами, действующими под руководством государства или по его указанию. Операции, проводимые такими акторами, могут спровоцировать применение понятия «вооруженного нападения» со всеми вытекающими последствиями для вовлеченных сторон.

Подчеркивается, что сегодня способности маскировать государственную принадлежность в информационном пространстве достаточно велики. Вместе с тем, доступные средства позволяют с высокой точностью идентифицировать источники опасности в информационном пространстве и оценивать деятельность той или иной стороны, исходя из складывающейся ситуации.

В целом следует отметить, что по большому числу вопросов юридического обеспечения применения силы в информационном пространстве мнение американских и европейских экспертов совпадают. Это позволяет говорить о том, что экспертное сообщество Запада выработало единое представление о применении силы в информационном пространстве. Данный факт ведет к серьезному переосмыслению ряда военно-политических оценок и станет отправной точкой активизации применения средств информационно-технического воздействия в ближайшие годы.

Материал поступил в редакцию 12. 02. 2014 г.