Секция «Международное право»

Проблемы применения норм и принципов международного гуманитарного права по отношению к кибератакам.

Научный руководитель – Ежова Татьяна Геннадьевна

Фицнер Виолетта Юрьевна

Студент (магистр)

Балтийский федеральный университет имени Иммануила Канта, Юридический институт, Калининград, Россия

E-mail: fitsner.violetta@yandex.ru

В настоящее время стремительное развитие компьютерных технологий поднимает ряд вопросов, касающихся применения существующих норм международного гуманитарного права. В частности,

1. Является ли кибератака «нападением» в соответствие с нормами МГП?

Большинство правил, касающихся ведения военных действий, содержат в себе термин «нападение», например, запрет нападения на гражданские лица и объекты [1]. Согласно части 1 статьи 49 Дополнительный протокола I, «нападения» означают акты насилия в отношении противника, независимо от того, совершаются ли они при наступлении или при обороне. Следовательно, возникает вопрос, при каких обстоятельствах кибератака будет считаться таким актом насилия.

Группа экспертов, принявшая Таллиннский руководство 2.0., определила, что кибероперация, которая, «как можно обоснованно предполагать, повлечет за собой ранения или гибель людей или ущерб, или повреждения объектов», должна считаться «нападением» по смыслу МГП [5]. Например, если кибератака становиться причиной отключения электричества в больнице, что приводит к смерти пациентов, такая атака подпадает под определение «нападение» [2]. Помимо физического ущерба, под ущербом следует понимать и выведение из строя того или иного объекта [4]. Однако, временный отказ в обслуживании системы, вызывающий только неудобства, не является нападением и, соответственно, не подпадает под действие правил ведения военных действий.

2. Применение принципа разграничения к кибер атакам.

Принцип разграничения предусматривает обязанность для сторон вооруженного конфликта всегда проводить различие между гражданским населением и комбатантами, а также между гражданскими объектами и военными объектам [1].

Во-первых, кибероперация может быть осуществлена только против комбатантов. Комбатантами являются лица, входящие в состав всех организованных вооруженных сил, групп и подразделений государства [1]. Также, гражданские лица, принимающие непосредственное участие в военных действиях, теряют свою защиту от ненападения *на тот период* [1].В отношении кибер атак, именно гражданские лица чаще всего совершают указанные операции [2]. Возникает вопрос, на какой период такие лица теряют защиту от ненападения, только ли на момент нажатия клавиши, которая активирует операцию?

Во-вторых, кибератака может быть направлена только против тех объектов, которые в силу своего характера, расположения, назначения или использования вносят эффективный вклад в военные действия [1]. Кибератаки представляют собой операции с целью

изменения, повреждения или уничтожения компьютерных данных или систем [6]. В связи с этим, командно-контрольные средства и радиолакационные волны будут являться военными объектами в силу своего характера. Однако, в контексте кибератак, множество объектов являются объектами двойного назначения. Например, подводные коммуникационные кабели и социальные сети используются как для военных, так и для гражданских целей [4], а, значит, могут быть атакованы. Таким образом, вопрос соблюдения другого принципа МГП, принципа пропорциональности, представляет особую актуальность.

3. Применение принципа пропорциональности к кибератакам.

В МГП запрещается нападение, которое, как можно полагать, повлечет за собой потери жизни среди гражданского населения, ранения гражданских лиц и ущерб гражданским объектам, которые были бы чрезмерны по отношению к конкретному и непосредственному военному преимуществу [1].

Кибероружие классифицируется как «несмертельное» оружие, так как, в отличие от конвенционного оружия, оно поражает системы и базы данных и не вызывает напрямую смерть людей и физические повреждения объектов. Можно предположить, что благодаря таким характеристикам, использование кибероружия сократит размеры «сопутствующего ущерба» среди гражданских лиц и объектов, и, следовательно, будет соответствовать принципу пропорциональности. Однако данный вывод является спорным.

В силу единства и взаимосвязанности киберпространства, при осуществлении атаки у оператора возникнут сложности при определении возможных последствий нападения [3]. Так, в 2010 г. произошла атака на Иранский завод по обогащению урана, в результате которой компьютерный вирус Stuxnet вывел из строя работающие центрифуги [6]. Кроме того, данный вирус поразил множество компьютерных систем жителей Ирана. Несмотря на то, что указанная операция не была проведена в рамках вооруженного конфликта, она представляет собой яркий пример непредсказуемых последствий от кибератак.

Источники и литература

1) Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов, от 8 июня 1977 г. (Протокол I) // Международный комитет красного креста URL: https://www.icrc.org/rus/resources/documents/misc/treaties-additional-protocol-1.htm.

2) Nasu H., McLaughlin R. New technologies and the Law of Armed Conflict. Canberra. 2014.

3) Radziwill Y. Cyber-attacks and the exploitable Imperfections of International Law. Boston. 2015.

4) Schmitt N. M. Peacetime Cyber Responses and Wartime Cyber Operations under International Law: an Analytical Vade Mecum. // Harvard National Security Journal. Cambridge. 2017. Vol. 8. P. 239-282.

5) Schmitt N. M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge. 2017.

6) Tsagourias N., Buchan R. Research Handbook on International Law and Cyberspace. Cheltenham. 2015