Секция «Актуальные вопросы современного международного права»

Международно-правовое регулирование кибероружия: проблемы и перспективы

Говалло Артём Сергеевич
Студент (бакалавр)
Севастопольский государственный университет, Юридический институт, Севастополь, Россия
E-mail: postinbox46@mail.ru

Современное общество невозможно представить без информационных технологий и сети «Интернет». Цифровизация естественным образом затронула все сферы функционирования государства и жизни его населения, будь то экономика, политика или право. Исключением не стала и военная сфера. Однако в отличие от большинства областей жизнедеятельности государства, информационные технологии не только имеют обеспечительный, вспомогательный характер, но и стали с некоторых пор самостоятельным, отдельным видом вооружения, так называемым «кибероружием». Ввиду того, что все больше сфер деятельности подвергаются цифровизации, масштаб киберугроз, кибератак, т.е. фактов применения кибероружия, неуклонно возрастает. Уже сегодня, ни одно государства самостоятельно не в состоянии справиться со всеми киберугрозами национальной безопасности, учитывая также международный характер этих посягательств. В этой связи, с целью недопущения произвольного, негуманного использования кибероружия в нарушение общепризнанных принципов и норм международного права в целом, и международного гуманитарного права в частности, актуальным является вопрос межгосударственного регулирования его правового статуса, контроля за распространением, правил разработки и применения, иных аспектов данного явления.

Для полноценного раскрытия настоящей темы необходимо рассмотреть понятие кибероружия и его особенности.

Так, в военной науке под кибероружием понимают вредоносное «программное обеспечение или оборудование для нанесения ущерба в киберпространстве» [1], т.е. любым цифровым устройствам и информационным системам. При этом, само киберпространство может быть, как сопряжено с реальной инфраструктурой (например, система электроснабжения города), так и находится исключительной в цифровой среде (например, информационные базы данных).

Характерными чертами кибероружия, в свою очередь, являются: специфическая среда применения, не имеющая физических границ (киберпространство), и как следствие - нематериальность самого оружия, неограниченность и относительно низкая стоимость распространения, мгновенность действия, скрытность источника применения и ряд других [1].

В настоящее время, несмотря на значение реальных и потенциальных угроз, положения о кибероружии содержатся в незначительном количестве нормативно-правовых актов. Например, в Соглашении между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009 г. К тому же, их положения не отражают реальной степени опасности предмета регулирования, а равно не устанавливают действенных механизмов противодействия.

Из вышеперечисленных особенностей вытекает проблематика установления международного контроля данного типа вооружений.

Мгновенность действия кибероружия означает невозможность превентивной обороны и оперативного реагирования на угрозу, а не на свершившуюся атаку. Также, эффективность противодействия как применению, так и распространению кибероружия не может быть перманентной, в связи с высокими темпами развития информационных технологий, а значит и самого кибероружия [2].

Из-за доступности и масштабируемости распространения, некоторые специалисты заявляют о невозможности создания режима контроля за кибервооружением по аналогии с существующими [2]. Следовательно, необходимо разрабатывать принципиально новые правовые концепции и механизмы нераспространения.

Скрытность применения, в свою очередь, ведет к проблеме идентификации лиц, причастных к кибератаками и невозможности юридического доказывания вины конкретных субъектов [3].

Существует угрозы, исходящие и от самого потенциального регулирования кибероружия. К таким относится угроза избыточного регулирования, ограничивающего свободу интернет-пространства, ущемляющего информационные права рядовых пользователей сети «Интернет» в ходе противодействия глобальным киберугрозам, что также является проблемой. Данное положение подтверждает острую необходимость реализации концепции «демилитаризации информационного пространства», поддерживаемой рядом стран [4].

Также не исключены риски злоупотребления правом на противодействие киберугрозам и превентивных кибератак по необоснованным подозрениям, ряд иных потенциально деструктивных ситуаций, оправдываемых на практике реализацией конкретных международно-правовых норм.

Несмотря на обилие проблематики в рамках рассматриваемой темы, в настоящее время, в отсутствие правового регулирования, исследователями данной области выдвигается ряд предложений.

Так, вместо труднореализуемого режима контроля за распространением кибероружия, предлагается ввести режим неприменения, т.е. международно-правового запрета на использование киберпространства в военных целях с соответствующими санкциями [2].

Ввиду известности фактов кибератак не только со стороны частных лиц, но и со стороны государств-субъектов международного права [5], целесообразным представляется введение международно-правовой ответственности за разработку, применение и распространение кибероружия.

Так или иначе, правила, институты и механизмы контроля за производством, распространением и применением кибероружия еще только предстоит разработать. Вероятно, в ближайшем будущем международное гуманитарное право пополнится договорами, регламентирующими различные аспекты кибероружия, в том числе его нераспространение и неприменение.

Источники и литература

1) Тиханычев О.В. Ограничение распространения кибероружия как фактор обеспечения безопасности в информационном мире // Вопросы безопасности. – 2018. – № 2. – С. 43-49.

2) Себекин С. Возможен ли режим контроля за распространением кибервооружений? Подходы России и США // Пути к миру и безопасности. – 2021. – № 2(61). – С. 139-152.

3) Барков А.В. Правовое обеспечение информационной безопасности: инструменты противодействия киберугрозам / А.В. Барков, А.С. Киселев // Журнал прикладных исследований. – 2022. – № 5-1. – С. 91-96.

4) Юдина Ю.А. Возможность применения средств обеспечения международной безопасности к информационному пространству // Актуальные проблемы российского права. – 2022. – Т. 17. – № 6(139). – С. 168-176.

5) О правовых инструментах реализации американской стратегии киберсдерживания / И.Н. Дылевский, С.И. Базылев, В. О. Запивахин [и др.] // Военная мысль. – 2021. – № 6. – С. 133-141.