УДК 341.1/8

Сикач Артём Сергеевич,
Студент 2 курса Юридической школы
Дальневосточного федерального университета
Россия, г. Владивосток

«КИБЕРНЕТИЧЕСКОЕ ОРУЖИЕ МАССОВОГО ПОРАЖЕНИЯ И МГП»

Аннотация: *В данной статье рассматривается роль кибернетического оружия массового поражения в международном гуманитарном праве. Актуальность данной темы заключается в том, что в последнее время во время вооружённых конфликтов между государствами возникает применение разных видов оружия массового поражения с целью нейтрализации государственного противника, а также в возможности получения полного контроля над наработками самого государства, связанные с развитием экономики, социальной и политической жизни общества. Одним из видов оружия массового поражения является кибернетическое оружие, потому что кибернетическое оружие играет роль в проведении нанесения ущерба информационным ресурсам и инфраструктуре противника с помощью информационных технологий, итогом которого может быть ущерб и разрушение, потеря и искажение данных, остановка или подмена целей работы систем. Автором приводятся примеры создания вооружённых сил в странах, в том числе и в России с целью противостояние противнику – государству его кибернетическому оружию. В результате проведённого исследования делается вывод о том, что кибернетическое оружие массового поражения сыграет не последнюю роль в вооружённом конфликте между государствами.*

Ключевые слова: *Кибернетическое оружие массового поражения, международное гуманитарное право, вооружённые конфликты, кибервойна, компьютерный вирус.*

Sikach Artem Sergeevich,
2nd year student of the Law School
of the Far Eastern Federal University
Russia, Vladivostok

Annotation: *This article examines the role of cybernetic weapons of mass destruction in international humanitarian law. The relevance of this topic lies in the fact that recently, during armed conflicts between states, the use of various types of weapons of mass destruction has arisen in order to neutralize a state enemy, as well as in the possibility of obtaining full control over the state's own developments related to the development of the economy, social and political life of society. One of the types of weapons of mass destruction is cybernetic weapons, because cybernetic weapons play a role in carrying out damage to information resources and infrastructure of the enemy with the help of information technologies, the result of which can be damage and destruction, loss and distortion of data, stopping or replacing the goals of the systems. The author gives examples of the creation of armed forces in countries, including Russia, in order to confront the enemy state with its cybernetic weapons. As a result of the conducted research, it is concluded that cybernetic weapons of mass destruction will play an important role in the armed conflict between states.*

Keywords: *Cybernetic weapons of mass destruction, international humanitarian law, armed conflicts, cyberwar, computer virus.*

Киберпространство становится объектом военных действия вместе с морей, с сушей, космосом и воздухом. Кибервойна является одним из

магистральных направлений революции в военном деле, разворачивающийся на наших глазах. Учитывая значимость и открытость цифровой инфраструктуры, государства осознают необходимость её защиты, с целью чего в рамках министерств обороны и специальных служб создаются соответствующие подразделения, предназначенные как для защиты от киберугроз, так и для проведения атак цифровой инфраструктуры. Например, Дональд Трамп – последний президент США – официально расширил полномочия Киберкомандования войск США (USCYBERCOM, U.S. Cyber Command), разрешив им осуществлять превентивное нападение на потенциальных противников[1]. Новые полномочия позволяют военным хакерам вести подрывную деятельность в сетях иных государств «на грани военных действий» - осуществлять шпионаж в компьютерных сетях, саботаж и диверсии в виде распространения вирусов и иных специальных программ.

В 2014 г. Указом Президента РФ В. В. Путина были сформированы Войска информационных операций, а в январе 2020 года объявлено о создании в вооружённых силах (ВС) России специальных подразделений, предназначенных для проведения информационных операций – о чём было сказано министром обороны Сергеем Шойгу[5].

Имеются кибернетические войска и в других странах. По неподтверждённым данным, бюджет кибервойск США составляет порядка 7 млрд долларов, а численность персонала превышает 9000 человек. Численность кибервойск КНР составляет порядка 20 000 человек с финансированием порядка 1,5 млрд долларов. Британия и Южная Корея тратят на кибербезопасность по 450 и 400 млн долларов соответственно. Российские кибервойска, предположительно включают порядка 1000 человек, а расходы составляют около 300 млн долларов. Возрастание возможности применения в вооруженном конфликте кибер-технологий актуализирует вопрос о применении к такого рода операциям норм международного гуманитарного права.

По мнению различных учёных, нормы МГП могут применяться только тогда, когда операции в кибернетическом пространстве ведутся в контексте вооружённого конфликта или в связи с ним[2]. Не вызывает возражений утверждение, что в случае проведения операции в киберпространстве в контексте вооруженного конфликта, они регулируются теми же нормами МГП, что и этот конфликт. Но целый ряд операций, характеризующихся как кибернетические военные действия, могут осуществляться не только в контексте вооруженных конфликтов[6]. Такой термин, как «кибер-атака» может ассоциироваться со способами военных действий, но операции, которые этим термином обозначают, могут проводятся и не во время вооруженного конфликта. Всем известен термин кибер-преступления, которые совершаются в повседневных ситуациях, которые не имеют ничего общего с войной.

Могут складываться ситуации, которые находятся между ситуациями существующих вооруженных конфликтов, которые ведутся традиционными методами, и кибер-операциями и ситуации, которые никак не являются вооруженным конфликтом. Классифицировать такие ситуации труднее. Например, так складывается ситуация, когда нападения на компьютерные сети являются единственными совершаемыми враждебными действиями или когда они остаются одиночными актами. Исследователи считают, что если нападение осуществлялось государством, оно может считаться международным вооруженным конфликтом. А если кибератаку осуществляет неправительственная организация против правительства, - можно ли такую ситуацию считать немеждународным вооруженным конфликтом? Ответ на вопрос, может международный вооруженный конфликт начаться в результате компьютерной атаки, зависит от следующих обстоятельств: 1) присваивается ли нападение на компьютерную сеть государству и 2) приравнивается ли оно к применению вооруженной силы.

Потенциальные деструктивные возможности компьютерных вирусов огромны, и они стремительно усиливаются по мере цифровизации окружающего мира. Все помнят обвинения США в адрес России о вмешательстве в американские выборы, а также обвинения в адрес Китая в краже интеллектуальной собственности[3]. Но манипуляция общественным сознанием и кража данных – лишь верхушка айсберга. Ряд технологий, таких, в частности, как фальсификация сообщений, способен сделать возможным манипулирование сознанием лидеров и населения неприятельской страны: распространять замешательство или недовольство путем тайного изменения официальных сообщений или новостей СМИ, путать или пугать руководителей государства фабрикацией ложной информации. В принципе эти действия не нарушают военное право. Однако длительно устанавливавшимся обычным правом и некоторыми конвенциями запрещены определенные акты предательства или «вероломства». Одно дело, скажем, угроза морского вторжения в Кувейт во время боевых действий в Персидском заливе. Есть основания признать ее актом, спланированным для того, чтобы сбить противника с толку, побудить его к опрометчивым шагам. Другое дело – акты вероломства, которые включают симулирование перемирия или капитуляции, ранения или неспособности, статуса гражданского населения или других статусов, обладающих защитой (нейтральные войска ООН) ради нанесения внезапного удара по врагу. Запрещено также и нападение с использованием форменной одежды противника.

Потенциальные результаты манипулирования сознанием могут быть достаточно серьезны. Некоторые наблюдатели, например, убеждены, что так называемое радио ненависти вызвало геноцид в Руанде и бывшей Югославии. Таким образом, использование пропаганды или обманных передач в эфире так, чтобы они стимулировали неограниченную гражданскую войну или даже геноцид, следует признать незаконным. Как полагает полковник Ричард Сжафрански, манипулирование народом противника в такой степени, что его

граждане или лидеры становятся оторванными от реальности, может быть не менее вредоносным, чем воздействие на другой народ через голод или каннибализм[4].

Но как же регулируется нормами международного гуманитарного права? Ведь его фундаментальный принцип заключается в том, что допустимые методы причинения вреда врагу не должны быть неограниченными. Однако это еще не означает, что оно стремится защищать от всех разновидностей ущерба, который причинят информационные атаки. Ведь государства с повышенным военным потенциалом разрабатывают новые технологии постоянно, а масштаб МГП является достаточно широким, чтобы учитывать и новые развития событий. МГП запрещает во время вооружённого конфликта использовать конкретные виды оружия массового поражения, например, биологического и химического оружия или противопехотных мин. МГП регулирует общими нормами способы и методы ведения войны, а также применение всех видов оружия. В статье 36 Дополнительного протокола I (ДП I) к Женевским конвенциям предусматривает, что: «при изучении, разработке, приобретении или принятии на вооружение новых видов оружия, средств или методов ведения войны Высокая Договаривающаяся Сторона должна определить, подпадает ли их применение, при некоторых или при всех обстоятельствах, под запрещения, содержащиеся в настоящем Протоколе или в каких – либо других нормах международного права, применяемых к Высокой Договаривающейся Стороне»[7]. Данная статья Дополнительного протокола I показывает, что кроме конкретного обстоятельства, наложенная данной нормой на государства – участников Дополнительного протокола I, нормы МГП применяются по отношению к новым технологиям.

Кажется очевидным, что они могут преступать законы войны. Так, паралич системы контроля воздушного движения способен вызвать катастрофы гражданских самолетов, а порча медицинской базы данных повлечет переливание несоответствующей группы крови гражданским лицам

и раненым солдатам. Возможны операции и с менее заметными результатами, например нарушение безопасности финансовой или социальной системы, открытие конфиденциальной персональной информации. Это не разновидность ущерба, против которого гуманитарное право, как предполагается, защитит население. Однако последствия сбоя работы банковских структур могут быть не менее болезненными, чем бомбардировка, повредившая жилые строения.

Двойственная природа многих телекоммуникационных сетей и большинства оборудования все больше усложняет вопрос о применимости гуманитарного права как ограничителя информационной войны. Размывание различий между военными и гражданскими системами стирает и границы между военными и гражданскими целями.

Во время кампании в Персидском заливе, например, коммерческие спутники обеспечивали функционирование четверти трансконтинентальных телекоммуникаций Центрального командования ВС США. Более того, американские вооруженные силы особенно зависят от невоенных систем для поставки и транспортировки. Таким образом, удары для решения военных задач необходимо будет направлять преимущественно на гражданские системы с причинением вреда зависимым от них мирным людям.

В 1995 году вице-адмирал Артур Кебровски заявил: «Между военными или гражданскими системами и технологиями не существует логического различия. Более того, техническое различие между эксплуатацией, атакой или защитой целей информационной войны также отсутствует».

Взаимозависимость и взаимосвязь гражданских и военных систем могут дальше усложнять определение гражданских и военных целей. Акции, направленные преимущественно против военных объектов, могут вызвать поражение гражданских систем, которые связаны с военными системами. Вирус, призванный вывести из строя военные системы врага, из-за невнимательности или в силу иных причин может проникнуть в гражданские

или дружественные системы. Более того, атаки на многофункциональные системы, которые в другом случае были бы законными целями, могут стать недопустимыми из-за опасности для гражданского населения, например, если они приведут к выбросу опасных веществ в атмосферу.

Из всего вышесказанного можно сделать вывод, что кибернетическое оружие массового поражения – это такое оружие, с помощью которого можно во время вооружённого конфликта нейтрализовать вооружение другого государства, а также его компьютерные технологии, чтобы можно было суметь получить полный контроль над другим государством.

Использованные источники:

1. Дрёге, К. Слезай с моего облака: кибернетическая война, международное гуманитарное право и защита гражданских лиц // Международный журнал Красного креста. 2014. т. 94. Избр. Ст. из № 885 – 888. С. 60.

2. Кибернетическое оружие массового поражения. URL: https://topwar.ru/181820-kiberneticheskoe-oruzhie-massovogo-porazhenija.html. (дата обращения: 12.04.2021).

3. Китай обвиняют в краже интеллектуальной собственности. URL: https://www.copyright.ru/ru/news/main/2020/01/27/china/. (дата обращения: 27.01.2020).

4. Информационная война и международное право. URL: https://vpk-news.ru/articles/9150. (дата обращения: 13.08.2012).

5. Россия ввела войска в интернет. URL: https://www.gazeta.ru/tech/2017/02/22_a_10539719.shtml. (дата обращения: 22.02.2017).

6. Гаркуша – Божко С. Ю. Кибер-атаки как новый способ ведения военных действий: возможность применения норм международного гуманитарного права // Фемида Science. 2017. № 4(6). С. 61 – 64.

7. Дополнительный протокол I к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов от 8 июня 1977 года. [Электронный ресурс]. URL: https://doc.mil.ru/documents/quick_search/more.htm?id=12093391%40egNPA (дата обращения: 18.01.2022).