ГУМАНИСТИЧЕСКИЕ АСПЕКТЫ КИБЕРВОЙН

Шипиловская Е.А.

Уральский государственный Юридический Университет(УрГЮУ)

Институт Прокуратуры группа 114Б

e-mail:bright_december2799@mail.ru

Аннотация: кибервойна - понятие, сопоставление с обычной войной. Проблема гуманистического аспекта кибер войны и правого регулирования.

Ключевые слова:кибервойна, гуманизация, информация, информатизация.

HUMANISTICASPECTSOFCYBERWAR

Shipilovskaya E.A.

”The Ural State Law University”

e-mail: bright_december2799@mail.ru

Abstract: Cyberwar is a concept, akin with common war. Thus cyber war as well as common war must achieve civilized forms by adoption of especial convention.

Keywords: Cyberwar, humanization, information.

Часто ли мы задумываемся о реальности войны? Нас учили с раннего детства, что это кровь, танки, самолеты, ракеты и прочие, сугубо материальные, физические атрибуты, из которых складывается всякая война.

Но к концу 20 века характер войн сильно изменился. И в самом деле, нерационально физически кого-то уничтожать (рискуя и собой), если можно попросту перепрограммировать своего возможного противника. Нерационально тратить дорогие боеприпасы, если достаточно правильно подобранных слов и образов (которые стоят очень дешево). На смену войнам приходят кибервойны.

Кибервойна (англ. Cyberwarfare) — противоборство (война) и противостояние в кибернетическом и коммуникационном

пространствах(киберпространстве), в том числе компьютерное противостояние в Интернете, а также противоборство с использованием высокотехнологичных и (или) массовых каналов коммуникации.

Что мы знаем о кибервоинах? Очень мало, нам трудно представить, что это такое, как она происходит и можно ли с ней бороться. И можно ли утверждать, что мы свидетели данного события. Парадокс заключается еще и в том, что само утверждение о существовании кибервойны может быть актом кибервойны (верно и обратное — молчание о войне тоже есть акт войны).

Кибервойна маскируется в потоках обыденной информации , официально не объявляется и проявляет себя в бесконечном множестве «фейков» (выдумок, не отличимых от правды), каждый из которых заранее объявляет фейками всех остальных. Основное средство поражения в кибервойнах — это принцип, который звучит так: все, что люди считают реальным, то реально по своим последствиям.

После двух самых кровавых войн в истории человечества (Первой и Второй мировой), а также десятков вооруженных конфликтов рангом поменьше, мировое сообщество осознало необходимость правового регулирования даже такого внеправового явления как война. Были приняты многочисленные конвенции и протоколы, гуманизирующие войны. Например: Конвенция о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении(от 13 января 1993 года), Конвенция по кассетным боеприпасам (19-30 мая 2008 года) и другие.

Представленные документы выполняют гуманистическую функцию нормы международного гуманитарного права, которые распространяются на военные действия на суше, на море и в воздухе, они применимы к наступлению и обороне. Их использование корректирует и расширяет содержание вооруженной борьбы. Военно-юридические знания становятся непосредственной теоретической основой вооруженной борьбы наряду с теориями стратегии, оперативного искусства и тактики.

Но этого нельзя сказать о кибервойнах, которые, будучи не менее эффективными и ожесточенными, на сегодняшний момент выведены из процесса гуманизации, особенно в части характера информационного воздействия. Конечно, Резолюция ООН, принятая Генеральной Ассамблеей от 31 января 2003 года, конечно, рассматривает гуманистическое направление культуры кибербезопасности. Но в данной резолюции регулируются по существу физические (или технические) элементы кибервойн — системы и сети. Вопросы лжеинформации не рассматриваются, хотя косвенно в них упоминается в пунктах a) осведомленность. Участники должны быть осведомлены о необходимости безопасности информационных систем и сетей и о том, что они могут сделать для повышения безопасности; b) ответственность. Участники отвечают за безопасность информационных систем и сетей сообразно с ролью каждого из них. Участники должны подвергать свои политику, практику, меры и процедуры регулярному обзору и оценивать, соответствуют ли они среде их применения; d) этика. Поскольку информационные системы и сети проникли во все уголки современного общества, участникам необходимо учитывать законные интересы других и признавать, что их действия или бездействие могут повредить другим.

Я хочу подчеркнуть, что документ принят в 2003 году и прошло уже 15 лет, за которые информатизация достигла своего пика. Элементы актуальны и в наше время, но требуют дополнения.

«Тихая» война несет за собой ужасные последствия. И требует регулирования со стороны международного сообщества. «Кто владеет информацией, тот владеет миром», - сказал Натан Ротшильд. Своим высказыванием автор хотел затронуть проблему значимости информации в бизнесе. А охватил им целое направление информационного века. Кибервойна все становится бессердечней, находиться в неведение – это одно из самых зловещих наказаний. Каждый человек должен иметь право на доступ истиной информации. Вербовка, проникновение в людской разум, закладка неправдивой информации, разве это гуманно? Я думаю, что нет.

Поэтому сегодня назрела необходимость создания документов, определяющих пределы искажения реальности, допустимых в самых ожесточенных кибервойнах.

Библиографический список:

1. И.Н. Сидоренко, Тотальная война: Феномен XXI века, 2016 год
2. Резолюция Генеральной Ассамблеи (ООН от 31.01.2003г)