ГИБРИДНАЯ ВОЙНА И ЦИФРОВОЙ ТЕРРОРИЗМ: ПОЛИТОЛОГИЧЕСКИЕ ТЕРМИНЫ В ЮРИСПРУДЕНЦИИ

М.А. Стародубцева
Алтайский государственный университет, г. Барнаул
email: starodubzewa@gmail.com

Аннотация. В статье поднимается вопрос о необходимости смешения юридических и политологических терминов, обозначающих гибридную войну и цифровой терроризм. Внедрение в традиционную войну цифровых технологий в публицистике часто называют «гибридной» войной. Однако необходимо отметить, что указанная концепция, как и цифровой терроризм – понятия, пришедшие из политологии, и к юриспруденции имеющие лишь косвенное отношение. При этом не стоит забывать о терминологической путанице между концепциями «гибридной» и «информационной» войн, «информационного оружия» и «цифрового терроризма». В политологической науке упомянутые термины до сих пор не имеют точного объяснения. Автор статьи приходит к выводу о том, что политологические термины не имеют общих точек соприкосновения с юриспруденцией.

Ключевые слова: гибридная война, цифровой терроризм, информационное оружие, юридический термин, политологическая концепция.

Изменение современной геополитической и геостратегической обстановки означает, в свою очередь, изменение военного искусства и философии. Это вызвано, прежде всего, глобализацией и цифровизацией, позволяющим легко менять интенсивность и стратегии конфликта, даже находясь за его пределами.

Собственно термин «гибридная война» впервые появляется в англоязычных публикациях с 2001 года [1, с. 128]. Любопытно отметить, что в первоначальном контексте он означал объявленную США «глобальную войну с терроризмом». Под гибридной войной понимается современный способ ведения военных действий, представляющий собой сочетание классических методов военных операций с партизанской войной, терроризмом, информационной войной (кибервойной), биологической и т.д. Примерно с 2014 г. данный термин введен в официальную политику России [2, с. 293].

Из всех методов ведения гибридной войны интерес представляет информационное противодействие, поскольку именно с его помощью происходит массовое распространение идеологических воззрений. Информационно – психологическое давление в гибридной войне является одним из основных методов и призвано достичь необходимого результата, используя достаточно скромные средства, такие как информационные вбросы для сдерживания потенциальной агрессии противника или формирования в общественном сознании образа «врага». Отмечается, что «гибридные» конфликты сочетают в себе «мягкие» действия, подготавливающие почву для «жесткого» вторжения уже на территорию атакуемого государства. Цель, в конечном счете, состоит в разрушении атакуемого государства изнутри, используя для этого подрыв идеологической базы государства, разрушение системы образования, разрыв поколенческих связей и традиций, разрушение системы морально – нравственных ценностей, хаотизацию экономики, искусственно подогреваемое недовольство масс, раскол меньшинств, создание условий, способствующих контролируемой и неконтролируемой миграции, подавлению гражданского сопротивления и разрушению критически важной инфраструктуры [2, с. 294]. В теории указанный результат достижим за счет использования масштабного информационно – психологического давления.

Именно здесь на первый план выходит информационный фактор гибридной войны, который, по мнению таких политологов, как О. А. Лаут, Г. Ш. Бибарсов и М.

А. Власенко, и называется полноценной «информационной войной» [2, с. 295]. Новые технологии позволяют достигать стратегических целей с помощью нетрадиционных и когнитивных эффектов (технологии социального влияния и манипулирования, информационное оружие, возможности значительного повреждения систем управления государством). Технологии, такие как социальные сети, позволили субъекту дистанционно влиять на все основные институты и инфраструктуру государства. Подобное влияние можно считать нетрадиционным вторжением на территорию атакуемой страны без использования прямой агрессии. Дистанционное, сетевое влияние сделало возможным внешне организованные и поддерживаемые движения сопротивления и терроризм, которые также могут достичь стратегических целей без насилия [3, с. 12]. Цепь дистанционно управляемых информационных процессов, способных осуществить информационно – психологическое воздействие на массы пользователей тех же социальных сетей может называться информационным оружием, как основным способом ведения информационной войны в контексте войны гибридной либо отдельно от нее. И, как уже указано в предыдущей главе, разновидностью информационного оружия выступает цифровой терроризм, отличный, прежде всего, по своим целям от остальной совокупности методов информационного давления.

В этом случае террористическим структурам отводится роль фактора дестабилизации внешней и внутренней жизни государства – противника, который сфокусированно добивается радикализации тех или иных групп населения, дискредитирует политику государства, оттягивает на себя ресурсы, в наиболее уязвимые для общества периоды выступает силой, которая окончательно должна подтолкнуть неустойчивую систему к ситуации коллапса и нестабильности [4, с. 108].

Управляемые по типу ИГИЛ проекты создают в современном мире условия для ведения терроризмом перманентной глобальной войны для создания ситуации политической и экономической неопределенности, политической нестабильности на планете, позволяющие инициатору процесса решать свои стратегические задачи. Направляя террористические группировки на те или иные объекты, те или иные государства, манипулятор получает возможность создавать информационный фон, способствующий включению или выключению государств в какие – либо процессы, осуществляет тотальное воздействие на обстановку в целом [5, с. 14].

Изменяющийся контекст мировых процессов, расстановка сил в глобальном масштабе и применение новых средств ведения противоборства фактически позволяют сегодня специалистам говорить о феномене нового терроризма как элемента стратегии ведения «гибридной войны» в цифровой сфере [6, с. 114].

Итак, кратко проанализированы широко транслируемые в современной политологии термины «гибридная», «информационная» войны, и «информационное оружие». «Гибридная» война порождает войну «информационную» как один из своих факторов, а та, в свою очередь, широко использует «информационное оружие». В исследовании предлагается придерживаться той точки зрения, согласно которой гибридная война и война информационная не могут полноценно существовать друг без друга, сливаясь в единое гибридно – информационное противостояние. В подобных рамках террористические организации, зачастую позиционируются как инструмент «гибридной» войны, внешне созданное и искусственно поддерживаемое образование внутри атакуемого государства, а цифровой терроризм, он же «цифровой терроризм» становится не более чем вариантом применения «информационного оружия».

В 2016 – 2017 гг. наблюдался первый опыт применения подобного оружия – всплеск активности суицидальных сообществ в социальных сетях. Субкультура самоубийств менее чем в полгода стала повсеместной и не утихает до сих пор.

Интернет – страницы игроков смертельных забав становились объектами поклонения, идеалом считался игрок, выполнивший последнее задание – собственно, самоубийство [7, с. 34]. Над молодыми людьми проводилась серьезнейшая работа с целью искусственного распада психики, при этом кураторы оказывали давление на недостатки детей – полнота, неуклюжесть, одиночество [8, с. 125]. Собственно, выполнение всех заданий «игры» было направлено именно на распад психики, формирование марионетки из жизнерадостного подростка. Стоит пристальней взглянуть на список заданий, и становится ясно, что их объединяет одно: особый язык намёков и символов. В этом суть любого программирования – запрограммированный человек расценивает самые, возможно, безобидные намёки как призыв к действию. Одно только то, что подросткам нужно было каждую ночь просыпаться в 4:20 ночи и смотреть психоделические видео со скачущими изображениями и искажениями звука, оказывает огромное влияние на их психологическое состояние. Ведь именно в это время уровень серотонина в организме понижен, что вызывает депрессивное воздействие на состояние человека, тревожность и уязвимость к внешнему воздействию. В результате чего у подростков происходило смешивание сна и реальности.

Исходя из предполагаемых мотивов деятельности кураторов, антиобщественной направленности их поведения, проявляющихся в особенностях переписки и записей разговоров, примеры которых приводятся ниже, предлагается определить данных лиц в категорию людей с аномалиями психики, не исключающими вменяемость, чаще всего, с истерической (истероидной) психопатией. Эта патология проявляется в виде театрального, демонстративного поведения, сопровождающаяся стремлением к совершению эпатажных, привлекающих внимание поступков. Личности с таким расстройством стремятся любым способом вызвать интерес к своей персоне. Подойдет даже ненависть или негодование, главное быть замеченным. «Цель истероида – быть замеченным. Ненасытное стремление к постоянному восхищению, жажда почитания своей персоны и беспредельный эгоцентризм можно считать характерными признаками данного расстройства»[9, с. 259]. Именно эти особенности поведения демонстрировал Филипп Лис, давая интервью изданию «Санкт – Петербург.ру». Приводятся некоторые отрывки для иллюстрации вышеуказанных тезисов: «Ты действительно подталкивал подростков к смерти? Да. Я действительно это делал. Не волнуйся, ты все поймешь. Все поймут. Они умирали счастливыми. Я дарил им то, чего у них не было в реальной жизни: тепло, понимание, связь» [9, с. 260]. На вопрос журналиста о том, с чего начались «группы смерти», Ф. Будейкин заявил, что «чистил общество» от людей, которые, якобы, не приносят никакой пользы. «Есть люди, а есть биомусор. Это те, кто не представляет никакой ценности для общества и несёт или принесёт обществу только вред. Я чистил наше общество от таких людей. Началось в 2013 году. Идею обдумывал на протяжении пяти лет. Можно сказать, готовился. Я продумывал концепцию проекта, конкретные уровни и этапы. Нужно было отделить нормальных от биомусора».

Указанная деятельность не признана террористической в российском законодательстве, но, как видится, имеет все ее признаки. Прежде всего, схожая модель вовлечения населения в «группу смерти» и в террористическое сообщество дает понять, что суицидальные группы выступали тренажером для потенциальных террористов. Наблюдалась идентичная технология вовлечения:

I этап. Знакомство. В случае суицидальных онлайн – сообществ это начало диалога с куратором.

II этап. Обещания. На этом этапе куратор начинал формировать у потенциального игрока представление об игре.

III этап. Группа риска. В случае суицидальных групп в подобную категорию попадали, преимущественно, подростки со сложной психологической обстановкой в семье либо испытывающие трудности в общении со сверстниками.

IV этап. Сообщество избранных. Куратор постепенно углублял у подростка представление о несправедливости жизни и неправильном поведении окружающих, подчеркивал и усиливал границу между подростком и реальным миром. Далее следовала сама «игра» [9, с. 260].

В результате анализа деятельности кураторов делается вывод о том, что «группы смерти» представляют собой успешный пример реализации воздействия методов социальной инженерии на пользователей социальных сетей в целях формирования искаженного восприятия действительности и террористического мировоззрения. Поэтому указанные сообщества предлагается определять как форму цифрового терроризма.

На почву нестабильной неокрепшей подростковой психики, сформированной на смертельных идеалах, в том числе суицидальных сообществ, наложилась волна скулшутинга в российских образовательных учреждениях. Указывается, что до 2014 г. данное явление в нашей действительности не встречалось. Предлагается выделить особенности, присущие как террористической идеологии, так и колумбайниане и суицидальным группам [10, с. 38]:

- основная цель – привлечение внимания демонстративно – насильственными действиями;
- активное вовлечение подростков и молодежи как лиц с неустойчивой психикой и несформированной гражданской позицией;
- безразличное отношение к жертвам, позиционирование носителя идеологии как высшего арбитра, правомочного отвечать насилием на обращенные против него действия;
- стремление к моральному оправданию насилия;
- тенденция перехода от конкретных целей к беспорядочным убийствам.

С точки зрения криминологии вышеизложенное дает основание относить идейное движение «Колумбайн» к терроризму, а массовое распространение его идеалов в интернет – сообществах – к форме цифрового терроризма. Указанный тезис частично подтвердил своим решением Верховный Суд РФ, признавший движение «Колумбайн» террористической организацией 2 февраля 2022 г[1].

Уголовная ответственность за склонение к совершению самоубийства или содействие совершению самоубийства в информационно – телекоммуникационных сетях (включая сеть «Интернет») определяется п. «д» ч. 3 ст. 110.1 УК РФ, а ответственность за организацию деятельности, направленной на побуждение к совершению самоубийства с использованием сети «Интернет» – ч. 2 ст. 110.2 УК РФ. Обе статьи введены Федеральным законом «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно – процессуального кодекса Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению» от 07.06.2017 N 120 – ФЗ[2].

[1] Верховный Суд Российской Федерации признал "Колумбайн" террористической организацией [Электронный ресурс]. Режим доступа: http://nac.gov.ru/hronika – sobytiy/verhovnyy – sud – rossiyskoy – federacii – priznal – kolumbayn.html (дата обращения: 18.11.2022).

[2] Федеральный закон "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно – процессуального кодекса Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению" от 07.06.2017 N 120 – ФЗ [Электронный ресурс] // Справ. – правовая система «КонсультантПлюс». URL: http://www.consultant.ru.

Федеральный закон от 18.12.2018 N 472 – ФЗ «О внесении изменений в статью 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» ввел новое основание включения сайта в «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», как содержащие информацию, распространение которой в Российской Федерации запрещено» – выявление информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья иных лиц[1]. При этом устанавливается, что блокировка таких сайтов должна производиться незамедлительно. Это нововведение фактически направлено на борьбу с распространением в сети «Интернет» идеологии движения «Колумбайн».

Указанные новеллы законодательства еще раз подтверждают вышеуказанный тезис о нецелесообразности введения в УК РФ отдельного признака либо состава цифрового терроризма. Тем более не требуется вводить отдельным признаком термин «гибридная война», как не имеющий отношения к юриспруденции.

Выделенные формы цифрового терроризма необходимо учитывать при формировании системы информационно–психологической безопасности (далее – ИПБ). Понятие психологической безопасности (далее – ПБ) встречается во многих исследованиях. Национальная ПБ понимается как защита граждан, отдельных групп, социальных групп, крупных объединений людей и населения страны в целом от негативных психологических воздействий. ПБ – это защита индивидуальной, групповой и общественной психики и, соответственно, социальных субъектов различного уровня общности, масштаба и системно – структурной и функциональной организации от воздействия информационных факторов, вызывающих дисфункциональные социальные процессы [11, с. 5]. Хотя в некоторых странах проводились исследования психологических аспектов международной безопасности, автором не найдено работ, которые бы определяли ИПБ. Исходя из приведенных определений, считается возможным определить ИПБ как защиту международных и внутригосударственных отношений от негативных информационно – психологических воздействий, связанных с различными факторами международного развития [12, с. 110]. К последним относятся целенаправленные усилия различных государственных, негосударственных и наднациональных субъектов, в частности, субъектов террористической деятельности, по созданию частичной/полной, локальной/глобальной, краткосрочной/долгосрочной и скрытой/открытой дестабилизации международной обстановки в целях получения конкурентных преимуществ, даже посредством физического устранения противника. Информационно–психологическая безопасность от информационно–психологического воздействия на личность означает, по сути, защиту рядовых пользователей от атак посредством социальной инженерии. А это является основной формой цифрового терроризма, как формы информационного оружия.

Итак, в работе рассмотрен понятийно – категориальный аппарат «информационной войны» и причины ее возникновения, и применения в ее рамках методов цифрового терроризма. Основной целью воздействия указанной системы являются рядовые пользователи информационно – коммуникационных сетей, в том

[1] Федеральный закон от 18.12.2018 N 472 – ФЗ «О внесении изменений в статью 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс] // Справ. – правовая система «КонсультантПлюс». URL: http://www.consultant.ru.

числе, сети «Интернет». Именно они выступают основной площадкой для распространения террористической идеологии и формирования террористического типа мировоззрения. Используя методы социальной инженерии, внедренные в информационное пространство, и грамотно выстраивая тактику массового вовлечения пользователей в террористические онлайн – сообщества идеологи терроризма, по сути, формируют силу, способную атаковать государство изнутри и самостоятельно разрушить собственную общественную систему. Указывается, что гибридно–информационное противостояние является политологическим термином и анализа с точки зрения юриспруденции не требует.

Библиографический список.

1. Комлева Н.А. Гибридная война: сущность и специфика // Известия Уральского федерального университета. Сер. 3, Общественные науки. 2017. Т. 12, № 3 (167). С. 128 – 137.
2. Романова В.А. Информационная составляющая гибридных войн современности // Государственное и муниципальное управление. Ученые записки СКАГС. 2015. № 2. С. 293–299.
3. Чекинов С.Г., Богданов С.А. Природа и содержание войны нового поколения. // Военная мысль 4 (2013). С.12 – 23
4. Рудаков А.В., Устинкин С.В. Трансформированная идентичность как ресурс международного терроризма и элемент стратегии «Гибридной войны» // Власть. 2016. №12. С. 103 – 108.
5. Чеботарев В.В. Концепт «новый терроризм»: за и против. – Дискуссия // Политематический журнал научных публикаций. 2015.Вып. 1(53). Январь. С. 14 – 21.
6. Добаев И.П., Добаев А.И. «Новый терроризм»: глобализация и социально – экономическое расслоение // Мировая экономика и международные отношения. 2009 № 5. С. 114 – 120.
7. Анисимова И.А. Преступления террористической направленности: сравнительные аспекты. Барнаул: Изд – во Алт. ун – та, 2021. С. 34.
8. Ильин Е.П. Дифференциальная психология профессиональной деятельности. Санкт-Петербург: Питер, 2016. 428 с.
9. Мазуров В.А., Стародубцева М.А. Новая волна «синих китов»: смертельные группы как тренажер для вербовщиков ИГИЛ // Аллея науки. 2017. Т. 3 №13. С. 259 – 263.
10. Пучнин А.В., Пучнина М.Ю. Идеология «колумбайн» как экстремистская и террористическая угроза национальной безопасности Российской Федерации // Общество и право. 2021. №2 (76). С. 38 – 43.
11. Безверхов, А.Г. О некоторых вопросах квалификации преступлений террористической направленности // Уголовное право. 2013. № 1. С. 4–10.
12. Шевченко, И.В. Уголовная ответственность за террористическую деятельность : монография. – Москва : Юрлитинформ, 2011. – 176 с.

HYBRID WAR AND DIGITAL TERRORISM: POLITICAL TERMS IN LAW

M.A. Starodubtseva
Altai State University, Barnaul
email: starodubzewa@gmail.com

Abstract. The article raises the question of the need to mix legal and political terms denoting hybrid war and digital terrorism. The introduction of digital technologies into traditional warfare is often called “hybrid” warfare in journalism. However, it should be noted that this concept, as well as digital terrorism, are concepts that came from political science and are only indirectly related to jurisprudence. At the same time, one should not

forget about the terminological confusion between the concepts of "hybrid" and "information" wars, "information weapons" and "digital terrorism". In political science, the mentioned terms still do not have an exact explanation. The author of the article comes to the conclusion that political science terms do not have common points of contact with jurisprudence.

Keywords: hybrid war, digital terrorism, information weapon, legal term, political science concept.