УДК130.2:004

О.А. Украинская

ФЕНОМЕН ИНФОРМАЦИОННОГО ТЕРРОРИЗМА В СОВРЕМЕННОМ ОБЩЕСТВЕ

*Стаття присвячена аналізу та узагальненню інформації щодо явища інформаційного тероризму. Аналізуються поняття «інформаційний тероризм», «інформаційна війна» та «кіберзлочинність». Зроблено висновок про необхідність розглядання феномена інформаційного тероризму як самостійного явища, народженого в умовах інформатизації та глобалізації.*

*Ключові слова: інформаційний тероризм, інформація, інформаційна зброя, інформаційний простір.*

*Статья посвящена обобщению и анализу информации о явлении информационного терроризма. Анализируются понятия «информационный терроризм», «информационная война» и «киберпреступность». Сделан вывод о необходимости рассмотрения феномена информационного терроризма как самостоятельного явления, рожденного в условиях информатизации и глобализации.*

*Ключевые слова: информационный терроризм, информация, информационное оружие, информационное пространство.*

*The article is dedicated to generalization and analysis of information on the phenomenon of information terrorism. The concepts of information terrorism, information war and cyber-criminality have been analysed. The conclusion has been drawn about necessity of regarding the phenomenon of information terrorism as independent phenomenon,arisen in the conditions of informatization and globalization.*

*Keywords: information terrorism, information, information weapon, information space.*

Современная цивилизация всё более быстрыми темпами приближается к тому этапу развития, который Элвин Тоффлер охарактеризовал как информационное общество, где главным фактором общественного развития является производство и использование информации [1].

Сегодня информация пронизывает практически все сферы жизни и деятельности, превращаясь в главный источник научно-технического и социально-экономического развития мирового сообщества. Технологии информационной эры обеспечивают возможность прямого манипулирования информацией, использования информационных потоков с целью направить развитие событий в определенном направлении. Наряду с привычным физическим пространством уже сформировалось и развивается виртуальное информационное пространство, от которого все больше становится зависимым человечество.

Формирование единого мирового информационного пространства превращается в глобальный фактор развития, который определяет основные направления общественного прогресса, информация становится важнейшим стратегическим ресурсом современного общества, а процесс информатизации – определяющей тенденцией современности.

Влияние процесса информатизации на социум достаточно противоречиво, что в некоторой степени обусловлено ускоряющимся развитием информационной сферы, на что указывает Мануэль Кастельс, утверждая, что скорость изменений в сфере информационных технологий неизменно растет [2]. Необъятное количество и доступность информации расширяют возможности человека в научной, образовательной, культурной, экономической сферах деятельности, но с другой стороны, информация становится одним из основных компонентов, обеспечивающих жизнедеятельность современных государств и может быть использована как мощное оружие, применяемое в террористических целях.

Во второй половине ХХ века явление терроризма стало повседневной реальностью для многих государств, что непосредственно обуславливает особую *актуальность* исследования данной проблемы в условиях повсеместной глобализации и информатизации общества.

Явление информационного терроризма ново, а потому *степень разработанности* данной проблематики невелика, в литературе ей уделено сравнительно мало внимания. Много говорится об информационных технологиях и международном терроризме, но важность совместного их исследования в настоящее время не в полной мере осознана.

Наибольший теоретический материал по вопросам информационного терроризма наработан американскими исследователями, признанными авторитетами в рассматриваемой области, Джоном Аркуиллой и Дэвидом Ронфельдтом. Серьезной разработкой проблематики информационного терроризма занимаются Г.Г. Почепцов, В.Н. Цыгичко, В.А. Мандрагеля, М. Требин, В.И. Головченко, В.П. Гондюл. Но работ, посвященных философскому анализу проблем, связанных с феноменом нового вида терроризма, практически нет. Исследования в этой области представлены немногочисленными статьями, посвященными, как правило, конкретным проявлениям информационного терроризма или отдельным вопросам информационной безопасности.

В связи с этим, первоочередной *задачей* является обобщение и анализ информации об информационном терроризме, и выявление сущности этого явления.

Становление феномена информационного терроризма как самостоятельного явления связано с появлением и развитием высоких технологий во второй половине ХХ столетия, хотя понятие терроризма, как механизма насаждения всеобщей паники и страха для достижения определенных социально-политических целей, имело место в истории на протяжении более чем двух тысяч лет.

Развитию и становлению информационного терроризма способствует множество факторов, но главным является развитие глобальной сети технических коммуникаций. Уязвимость и эффект даже от наименьших сбоев в функционировании которых, делает их главным объектом террористических акций.

Также немаловажную роль в становлении информационного терроризма, по мнению Ю. Марченко, играет распространение демократических принципов свобод (свободы передвижения, свободы слова и информации и др.) и симбиоз глобализации и локализации, который способствует использованию глобальных сетей в достижении локальных целей [3, с. 64].

Для более глубокого исследования проблемы информационного терроризма, необходимо уточнить смыслы, которые вкладываются в такие понятия как «информационный терроризм», «информационная война», «информационное пространство» «киберпреступность», «компьютерные преступления», чтобы отграничить их друг от друга и от смежных понятий.

Так, исследователи проблем терроризма часто не разделяют понятия «киберпреступность» и «кибертерроризм». Рассматривая киберпреступление как одно из проявлений международного терроризма, авторы [4] не выделяют кибертерроризм как самостоятельное явление, а определяют его как одно из проявлений информационных угроз современности. Но с данной позицией можно не согласиться, так как киберпреступление может являться лишь отдельным проявлением террористической деятельности, но никак не подменять понятие кибертерроризма.

Под термином «киберпреступность» будем понимать любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, понятие киберпреступности распространяется на все виды преступлений, совершенных в информационно-телекоммуникационной сфере, где информация, информационные ресурсы, информационная техника могут являться целью преступных посягательств, средой, в которой совершаются правонарушения, и средством или орудием преступления.

Можно выделить четыре типа компьютерных преступлений «в чистом виде»: незаконный доступ к компьютерной системе либо ее части; вмешательство в компьютерные системы (противоправное препятствование функционированию компьютерной системы); незаконный перехват не предназначенных для общественности компьютерных данных; вмешательство в компьютерные данные (противоправное повреждение, удаление, изменение либо пресечение компьютерных данных).

Именно эти четыре вида преступлений являются собственно «компьютерными», остальные – это либо связанные с компьютером (computer-related), либо совершаемые с помощью компьютера преступления (computer-facilitated). К ним относятся: преступления, в которых компьютер является орудием (электронные хищения, мошенничества и т.п.); деяния, при совершении которых компьютер является интеллектуальным средством (например, размещение на сайтах детской порнографии, информации, разжигающей национальную, расcовую, религиозную вражду и т.д.).

Таким образом, преступления в киберпространстве, а также преступления, в которых компьютер и компьютерные системы являются лишь орудием, могут выступать как самостоятельные явления, но в то же время они могут являться и проявлениями более масштабного явления – информационного терроризма.

Определение понятия «информационный терроризм» – достаточно сложная задача, так как до сих пор не существует общепринятого определения этого явления, несмотря на то, что учеными и правительственными организациями предложены сотни его дефиниций. Так, в связи неопределенностью в определении понятия «информационного терроризма» нелегко установить четкие грани между информационным терроризмом и информационной войной.

В отличие от информационного терроризма и компьютерных преступлений проявления информационной войны могут даже не являться нарушением закона.

Информационная война, по определению И.И. Завадского, состоит из действий, предпринимаемых для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем [5, с. 12]. В данном определении информационная война рассматривается как противоборство в политической сфере, что делает неполным это определение, так как ведение информационной войны не бывает обособленным, а подразумевает всеобъемлющую и целостную стратегию, согласованную деятельность по использованию информации как оружия для достижения определенных целей, в равной степени как в политической, так и в экономической и социальной сферах.

Информационные войны не являются изобретением последних десятилетий. На протяжении всей истории человечества войны сопровождались стремлением ввести противника в заблуждение, распространить деморализирующие его слухи, запугать, заставит отказаться от дальнейшей борьбы. Значительное количество специальных процедур и приемов достижения политических целей без вступления в открытую вооруженную борьбу были разработаны ещё тысячи лет назад [6, с. 453-462]. Но основной задачей информационных войн остается – манипулирование общественным сознанием, которое так же является и определяющей характеристикой информационного терроризма.

Информационный терроризм отличается от указанных форм воздействия на информационное пространство, прежде всего своими целями, которые остаются свойственными политическому терроризму. Средства осуществления информационно-террористических действий могут варьироваться в широких пределах и включать все виды современного информационного оружия. В то же время тактика и приемы его применения существенно отличаются от тактики в информационной войне.

Информационный терроризм можно определить как форму негативного воздействия на личность, общество и государство всеми видами информации, или, другими словами, манипулирование общественным сознанием посредством информационных технологий для достижения определенных целей. Он осуществляется преимущественно в областях, охватывающих политические, философские, правовые, эстетические, религиозные и другие взгляды – там, где ведется борьба идей.

Этот новый вид терроризма реализуется в информационном пространстве, представляющем собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Информационное пространство имеет существенные особенности, которые кардинально отличают ее от других компонентов среды обитания человека: неисчерпаемость и восполняемость информационных ресурсов, возможность их быстрого копирования, перемещения больших объемов практически без потерь, с высокой скоростью и на огромные расстояния, компактность источников и носителей информации и др. [7, с. 50].

Информационное пространство дает не только огромные возможности развитию науки и бизнеса, культуры и образования, экономики и социальной сферы государства, но и делает все более уязвимым как отдельного человека, так и государство и общество в целом, превращая информацию в мощное оружие.

Точного, общепринятого определения понятия «информационное оружие» нет. Известно, что впервые оно стало употребляться в американских военных кругах в 1991 году после окончания войны в Персидском заливе. Осложняет вопрос то обстоятельство, что информационные технологии большей своей частью выступают как технологии двойного или даже вообще невоенного назначения, то есть они первоначально появляются и главным образом задействованы в гражданском секторе, и лишь потом (или на время) используются как оружие.

Наиболее полное определение понятия «информационное оружие» предложено в [4, с. 14], где оно определяется как комплекс мероприятий, методов и технологий, направленных на установление контроля над информационными структурами потенциального противника, вмешательство в работу его систем управления с целью уничтожения или модификации данных, дезинформации, распространения информации специального назначения, а также, как совокупность средств влияния на сознание и психологическое состояние политических и военных структур, спецслужб и населения. Но и это определение требует разъяснения. Из данного определения можно сделать вывод, что с точки зрения цели использования и объекта воздействия, информационное оружие можно рассматривать как: а) набор технических средств, используемых для влияния на информационно-техническую инфраструктуру; б) совокупность средств воздействия на психику и сознание людей.

В содержательном плане информационное оружие – это специально подобранная информация, под воздействием которой происходят изменения информационно – коммуникативных процессов в различных информационных системах (физических, биологических, социальных и др.) в соответствии с замыслом субъектов его применения, в качестве которых могут выступать: государство, его специальные службы, международные или национальные террористические центры и организации, политические течения и партии экстремистского толка, группы граждан и даже отдельные лица, стремящиеся достичь своих целей с применением методов террора.

Среди принципов применения информационного оружия принято выделять внезапность, многоканальность, скрытность, системность, цикличность [8].

Обычно информационное оружие классифицируют по методам воздействия на информационную инфраструктуру: физическим, радиоэлектронным, информационным, программным.

Физические методы воздействия на информационную инфраструктуру могут быть осуществлены средствами минирования и подрыва, боеприпасами с головкой самонаведения на радиоизлучение, специализированными аккумуляторными батареями генерации импульса высокого напряжения, средствами генерации электромагнитного импульса (МГД-генераторами), средства летального или нелетального воздействия на персонал и др.

Радиоэлектронные методы реализуются средствами радиоэлектронного подавления и радиоэлектронной разведки, негласного съема аудио- и видеоинформации в помещениях, средствами генерации речи конкретного человека в целях дезинформации, а также средствами подавления радиоэлектронных средств помехами, имитирующими естественные отказы аппаратуры.

Информационные методы реализуются всей совокупностью средств массовой информации и глобальных информационных сетей.

Средствами реализации программных методов являются программные вирусы, программные и аппаратные закладки, а также специальные средства вскрытия защиты и проникновения в информационные сети. Эти средства являются наиболее перспективными, и понятие «информационное оружие» в большей степени относится именно к этим средствам.

Программные средства как разновидность информационного оружия являются наиболее доступными для разработки и применения в достижении своих целей террористическими организациями.

Основными особенностями нового поколения вооружений становятся кардинальное повышение точности, дальности и мощности действия, а также резкое увеличение возможностей и возрастание качественных характеристик разведки и систем сбора и обработки информации. Одним из важнейших факторов повышения качества современных систем управления является возможность сверхбыстрой передачи большого количества информации, что способствует обеспечению адекватности оценивания обстановки и принятия управленческих решений.

К характерным чертам информационного оружия можно отнести его качественную универсальность, радикальность воздействия, доступность. Оно отличается широким выбором времени и места применения. Для его приведения в действие не требуется больших армий, что делает информационные атаки сравнительно экономичными. Его применение носит обезличенный характер, легко маскируется под обычную деятельность. Одновременно трудно определить «обратный адрес» и национальную принадлежность террориста. Информационное оружие не знает географических расстояний, подрывает традиционное понятие государственных границ, делая их технологически проницаемыми. Осложняется возможность противодействия информационной агрессии в связи с отсутствием систем и методик, оценивающих угрозу нападения и заранее предупреждающих об атаке, что делает информационное оружие еще более эффективным.

Но все же главное в тактике информационного терроризма состоит в том, чтобы террористический акт стал широко известен населению и получил общественный резонанс, для чего всесторонне используются средства массовой информации и возможности «всемирной паутины» Интернет.

Террористы используют открытость Интернета для дискредитации правительств и государств, размещения сайтов террористической направленности, порчи и разрушения ключевых систем путем внесения в них фальсифицированных данных или постоянного вывода этих систем из рабочего состояния, что порождает страх и тревогу, и является своего рода дополнением к традиционному виду терроризма.

Информационный терроризм имеет в своем арсенале широкий спектр форм и методов террористической деятельности, их эффективность определяется такими особенностями информационной инфраструктуры как простота и дешевизна осуществления доступа к информационной инфраструктуре, размытость границ информационной инфраструктуры и, как следствие, невозможность какого-то четкого разграничения между внутренними и внешними источниками угроз.

Возможность искажения информации в информационной инфраструктуре позволяет управлять восприятием и манипулировать общественным сознанием. Таким образом, Интернет и СМИ служат средством распространения пропагандистских материалов различных террористических групп, не соответствующих действительности, но способствующих развитию террористической деятельности. Так, недостаток информации относительно реальных и потенциальных угроз информационного терроризма, необычайная сложность задач тактического предупреждения и оценки реального или вероятного ущерба, делает атаки террористов все более непредсказуемыми, а значит все более эффективными.

Таким образом, можно сделать *вывод*, что использованию информационно-кибернетических технологий в террористических целях способствуют, с одной стороны, простота и относительная дешевизна доступа к средствам связи и передачи данных, космополитизм глобальных информационных сетей, а с другой, – уязвимость мировых информационных ресурсов и инфраструктуры. Развитие технических средств нового поколения, которые способны эффективно воздействовать как на психику и сознание людей, так и на информационно – техническую инфраструктуру, вызывают необходимость активной разработки проблематики информационной безопасности личности, общества и государства, что невозможно без тщательного рассмотрения нового вида терроризма, рожденного в условиях тотальной глобализации и информатизации.

Перечень ссылок

1. Тоффлер Э. Третья волна. – М.: ООО «Издательство АСТ», 2002. – 776 с.
2. Castells Manuel The Rise of the Network Society. – 2nd ed.:Blackwell Publishing, 2000. – 624 p.
3. Марченко Ю. На тлі ціннісної кризи. Тероризм: анатомія витоків // Політика і час. – 2003. – №12. – с. 61-66.
4. Головченко В.І., Гондюл В.П., Зернецька О.В. та ін. Міжнародна інформаційна безпека: сучасні виклики та загрози. – К.: Центр вільної преси, 2006. – 915 с.
5. Завадский И.И. Информационная война – что это такое? // Защита информации. – 1996. – №4. – с. 10-18.
6. Мандрагеля В.А. Причини та характер воєн (збройних конфліктів): філософсько-соціологічний аналіз. – К.: Ін-т вищої освіти АПН України, 2003. – 569 с.
7. Андреев В.Г. Оружие и война: новые тенденции развития // Военная мысль. – 1999. – №3. – с.48-56.
8. Синчук Ю. Методы ведения современных войн. Информационное противоборство // Воин России. – 2000. – №8 //http://ebiblioteka.ru/sources/article.jsp?id=2464198.

Рецензент: д. філос. н. Штанько В.І.