Козориз, Н. Л. Об информационной среде противодействия терроризму / Н. Л. Козориз // Право.by. — 2014. — № 2. — С. 102—107.

ОБ ИНФОРМАЦИОННОЙ СРЕДЕ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ

THE INFORMATION ENVIRONMENT OF THE COUNTER-TERRORISM

КОЗОРИЗ Н.Л., доцент кафедры военной администрации, административного и финансового права Военного университета Министерства обороны Российской Федерации, кандидат философских наук, кандидат юридических наук, доцент

В статье раскрываются геополитические последствия информатизации во второй половине XX века, которые привели к появлению возможностей глобального воздействия на мировое, региональное или государственное информационное пространство, влияющие на правовое регулирование в глобальном информационном пространстве.

Выделяются информационное пиратство, информационный криминал и информационный терроризм как одни из наиболее опасных форм воздействия на киберпространство, требующих в том числе и правового регулирования.

The article describes the geopolitical consequences of information in the second half of the 20th century, which led to the emergence of opportunities for a global response to a global, regional or public information space, affecting the legal regulation in the global information space.

Information piracy, information crime and terrorism information stand out as one of the most dangerous forms of impact on the cyberspace, require, among other things, and legal regulation.

В политических системах любых типов информация выступает как ресурс власти, орудие борьбы или инструмент управления. В обществе наряду с законодательной, исполнительной и судебной властями выделяют четвертую, хотя и неофициальную, информационную власть, ставшую активной социально-политической силой современного общества. И даже типы политической власти – бюрократия или участие, тоталитаризм или демократия, накладывая свои особенности на осуществление информационной власти, принципиально не изменяют ее роль и значение в политической системе общества. Эту аксиому хорошо усвоил международный терроризм, природа и механизмы функционирования которого помимо других оснований тесно связаны с информационными процессами в обществе, а его преступная практика откровенно паразитирует на них.

Законодательно терроризм определяется как «идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий» [1, ст. 3].

В условиях социальной модернизации (теория роста) политика активно вмешивается в социально-экономические отношения, рассматривая их как механизм мобилизации природных, социальных и информационных ресурсов развития. Более того, накопление ресурсов становится одной из приоритетных функций государственной власти. Вместе с тем терроризм как политическое явление становится новым внегосударственным и нелегитимным способом перераспределения жизненно важных ресурсов, будь то рынки, деньги, нефть, территории, рабочая сила, влияние (политическое, экономическое, духовное и др.), технологии или информация.

Под влиянием мировой тенденции глобализации среди факторов, провоцирующих экстремизм и терроризм, возрастает роль информационных процессов и противоречий. На уровне политики государств это может проявляться в агрессивных идеологических установках, доктринах, авантюрных решениях и военных амбициях, провокационном или изоляционистском внешнеполитическом курсе (Северная Корея, Куба, Тайвань, Иран, Ирак, Пакистан). Кроме того, как показала практика, на этой почве могут появляться наднациональные, внегосударственные силовые структуры, ведущие террористическую войну против своих правительств, других стран или международных сообществ.

Геополитические последствия информатизации во второй половине XX века привели к появлению возможностей глобального воздействия на мировое, региональное или государственное информационное пространство. Это связано с возрастающей зависимостью современного общества от развития его информационной инфраструктуры (информационные ресурсы и системы, учреждения и организации, специалисты информационного профиля, системы связи и управления, телекоммуникационные средства и т.д.). Сегодня аналитики отмечают множественность форм системного воздействия на единое информационное пространство государства – информационное пиратство, информационный криминал, информационный терроризм и другое, в которых немалую роль играет правовой нигилизм.

Информационное пиратство представляет собой практику противоправного использования нелицензионных и несертифицированных информационных продуктов, а также присвоения интеллектуальной собственности. Помимо чисто коммерческих и юридических последствий пиратство в инфосфере – серьезная проблема информационной безопасности политических систем, так как оно способствует несанкционированному доступу к конфиденциальной государственной, экономической, научной, военной информации [4].

Информационный криминал – это действия отдельных лиц, групп или криминальных сообществ, направленные на взлом защиты, скрытное проникновение в информационные системы, хищение, искажение или уничтожение конфиденциальной информации с преступными целями. Типичные представители информационного криминала: «хакеры», «крэкеры», «фрикеры» – взломщики телекоммуникационных систем, воры, мошенники, злоумышленники и шпионы. Их действия часто носят откровенно криминальный характер и преследуются в уголовном порядке.

Одна из наиболее опасных форм воздействия на киберпространство – информационный терроризм. Он представляет собой специфический вид террористической деятельности, информационный способ осуществления или угрозы насилия в целях принуждения выполнения условий террористов посредством использования и (или) вывода из строя элементов информационной инфраструктуры государства. Наиболее вероятными приемами информационного терроризма в киберпространстве могут быть: искажение или модификация программного обеспечения и информации в информационных системах государства; угроза раскрытия информации, содержащей государственную и военную тайну; ложная угроза (шантаж) террористического акта с целью спровоцировать серьезные экономические или политические последствия; захват каналов СМИ в целях обращения террористов к общественности, выдвижения ультиматума или пропаганды экстремистских идей; уничтожение или нарушение нормальной работы линий связи, сетей электропитания, узлов коммутации; воздействие (насилие, шантаж, угроза, подкуп) на специалистов информационных и телекоммуникационных систем; кража или уничтожение информационного, программного и технического ресурсов. В соответствии с Федеральным законом Российской Федерации от 6 марта 2006 года «О противодействии терроризму» [1, ст. 11, пункт 3] в определенных случаях осуществляется:

ведение контроля телефонных переговоров и иной информации, передаваемой по каналам телекоммуникационных систем, а также осуществление поиска на каналах

электрической связи и в почтовых отправлениях в целях выявления информации об обстоятельствах совершения террористического акта, о лицах, его подготовивших и совершивших, и в целях предупреждения совершения других террористических актов;

приостановление оказания услуг связи юридическим и физическим лицам или ограничение использования сетей связи и средств связи.

В международных делах страны-лидеры, прежде всего США, нередко демонстрируют военно-полицейские формы поведения (операция НАТО в Косово без санкции ООН, бомбовые удары США по Ираку, информационно-сетевая атака в Сирии и т.д.) и тем самым провоцируют проявление экстремизма и терроризма. Примером новых политических технологий, повышающих легитимность применения насилия в обход принципа неприменения силы в международных отношениях, может быть доктрина так называемой «гуманитарной интервенции». Она понимается как вооруженное вмешательство с целью защиты «прав человека». Теоретически доктрина была обоснована в 1992 году в Нидерландах, а впервые практически реализована НАТО в Югославии (Косово). Теперь она реализуется в Афганистане. Сущность ее состоит в том, что одно государство или группа государств, оценивая ситуацию в другом государстве как «гуманитарную катастрофу», присваивают себе право по собственной инициативе и без санкции Совета Безопасности ООН вмешиваться в дела другого государства и применять вооруженную силу под предлогом защиты прав человека.

В гуманитарной интервенции исключительно высокая роль отводится информационным факторам в триединой функции «миротворчества»: принуждение к миру; обеспечение избирательного военного вмешательства; удержание международного политического контроля над ситуацией в государстве, подвергшемся «гуманитарной интервенции», до «восстановления прав человека». При этом субъекты интервенции самостоятельно определяют необходимость, масштабы и длительность военного присутствия в тех или иных регионах мира. Проще говоря, в массовом сознании с помощью средств массовой информации и сетевых технологий создается виртуальный образ «гуманитарной катастрофы» или так называемый «информационный повод», под предлогом которых осуществляется военно-политическое вмешательство (акции или операции).

Международный опыт последнего десятилетия красноречиво убеждает, что гуманитарная интервенция есть не что иное, как новое и достаточно эффективное средство современной геополитики, основанное на комбинировании военных и невоенных средств достижения, в первую очередь, политических и экономических целей. Контроль над геополитическим пространством и жизненно важными ресурсами осуществляется уже не столько посредством вооруженного захвата чужих территорий, сколько благодаря информационному проникновению, экономическим санкциям, локальному военному присутствию, насильственному свержению неугодного правительства и установлению лояльного общественно-политического режима, идеологической экспансии в культурное пространство других государств.

Вместе с тем диктат, исходящий из центров силы, провоцирует поиск субъектов международных отношений притесняемыми «странами-изгоями» и даже экстремистскими организациями несимметричных ответов на военно-информационные вызовы сильных мира сего. Террористическая активность как насильственная форма реакции-протеста «оскорбленных» в Израиле и США – яркое тому подтверждение. Международный терроризм, стремясь заполучить новейшие вооружения, в том числе оружие массового поражения, рассчитывает не столько на военный результат, сколько на информационно-политический эффект от обладания им, применения или угрозы применения. Отсюда появляются новые его разновидности – ядерный, химический, биологический, информационный терроризм.

Международный терроризм не только обеспечивается информационно (с помощью средств массовой информации, новых информационных технологий и PR-технологий). Характерно, что роль информационных ресурсов и технологий как ключевого фактора в подготовке и проведении террористических актов весомо возрастает. Здесь уместна

историческая аналогия: фашисты возводили пропаганду насилия и террора в ранг своей идеологии и политики. В годы Второй мировой войны в фашистской Германии особой популярностью пользовался немецкий радиовещатель Ганс Фриче, превзошедший в радиопропаганде британскую Би-би-си. В Нюрнберге он был приговорен к смерти как фашистский преступник, и это стало знаковым событием. Таким образом, была дана суровая оценка фашистскому информационно-пропагандистскому террору, ставшему частью не только стратегии ведения войны, но и военной политики в целом.

К сожалению, в теории и практике политики России не учитываются в должной мере информационные основания терроризма, значительно обусловливающие международный характер его организации. Облик террористической войны должен быть предметом глубокого научного анализа, на основании которого только и может быть определена конкретная политика России, направленная против международного терроризма.

Международная политика США на рубеже XX–XXI веков в основном сводилась к войнам с социальной доминантой [2, с. 64]. Они ведутся уже не столько за территории и ресурсы, сколько за национальные ценности. Главными объектами нападения в них оказываются общественное сознание, духовно-нравственные ценности (цивилизационные устои) и общественные институты (политическая система, религия, идеология, образ жизни и т.д.). Не случайно 11 сентября 2001 г. террористы для атаки в США избрали символы американского процветания и могущества – Международный торговый центр и Пентагон. Терроризм как социально-политическое явление ведет вооруженную борьбу с обществом, по всем признакам соответствующую определению войны с социальной доминантой. Может быть поэтому не найдено пока эффективное противоядие в борьбе против террора?

Диалектика мирового развития такова, что за глобальный прогресс человечество стало платить и более дорогую цену – глобальными социально-экономическими, политическими и экологическими потрясениями. Одно из тяжелейших среди них – международный терроризм. Словари трактуют террор (от лат. terror – страх, ужас) как угрозу насилием, запугивание, подавление противников насильственными мерами, а терроризм – как политику устрашения или тактику террора [5, с. 605].

Во-первых, террор – это действия, рассчитанные на массовое смятение, деморализацию населения и в конечном итоге на дестабилизацию обстановки в стране или регионе. Следовательно, террор – это сугубо политическое средство.

Во-вторых, террор предполагает широкую огласку относительно его ужасных последствий («чем хуже, тем лучше»), иначе как посеешь страх в сознании массы людей, как их запугаешь? Таким образом, неотъемлемым свойством террора является публичность, которая ассоциируется с демонстративным вызовом и возмущением общественности, шумихой в средствах массовой информации, изменением общественного мнения, активизацией внутренней оппозиции, международным резонансом, что приводит в движение и отвлекает мощные информационные ресурсы общества от решения конструктивных задач.

В-третьих, истинная цель террора состоит не в достижении военной победы над противником, а в подавлении его коллективной воли насильственными действиями или угрозой насилия, то есть в достижении, пусть даже кратковременного, морально-психологического превосходства. Перенос целей террора в «четвертое измерение» (в духовную сферу) объективно придает ему статус средства информационно-психологической войны (борьбы).

В-четвертых, субъект террора в момент своего осуществления (а все чаще и после него), как правило, не идентифицирован. Анонимность террористов обусловлена, с одной стороны, асимметричным характером тактики их борьбы и несопоставимостью их силовых потенциалов с государственными, а с другой – субъект-субъектным характером их отношений с жертвой.

Другими словами, источники террора в большинстве случаев – это субъекты политики в своих же государствах. Так, террористический режим Дудаева в Чечне стал

следствием деструктивной национальной политики российских «реформаторов первой волны», против которых он впоследствии и направил острие своего террора. Усама бен Ладен, в свою очередь, был взращен американскими и пакистанскими спецслужбами для организации борьбы в Афганистане с СССР, но после распада последнего обратил свой гнев в адрес США.

Отмечая данные черты современного терроризма, следует обратить внимание на ряд его особенностей:

терроризм приобрел международный характер и особую живучесть благодаря широкому распространению в мире информационных технологий, на основе которых стали возникать транснациональные преступные сообщества с сетевой структурой организации (по принципу паутины). Для них характерны единые центры, но автономный способ существования периферийных преступных группировок;

питательной средой терроризма является информационная среда общества, а составной его частью – информационные технологии, несущие в массы людей страх и ужас, с помощью которых террор стремится к достижению преступных целей;

явление терроризма становится новым виртуальным фактором в политической реальности – сила воздействия на общественное сознание, политические институты и решения правительств определяется силой и направленностью вызываемого общественного резонанса (объекты террора выбираются по принципу максимального информационного эффекта).

Все больше аналитиков выделяют новый тип современной войны, которую условно называют террористической. Например, США считают террористические акты 11 сентября 2001 г. «действиями войны» против цивилизованного мира. В основных чертах она напоминает идею «мятежевойны» Е. Месснера. Анализ показывает, что ее главными признаками являются следующие особенности.

1. Противник у государства чаще всего «невидимый», распределенный, рассредоточенный по стране или миру и действует анонимно, несимметрично, что делает неэффективным применение против него традиционных форм, методов и средств вооруженной борьбы. Такой противник предстает в виде наднациональных или негосударственных силовых структур (так называемой «третьей силы»), которые формируются по сетевому принципу.

2. Борьба с «третьей силой» требует от государства создания специальных антитеррористических формирований (группировок войск, спецназа, разведки, спецслужб, подразделений информационной борьбы и т.д.), широко применяющих новейшие информационные технологии и нетрадиционные способы ведения войны.

3. Линия фронта террористической войны «проходит» через общественное мнение и сознание, поэтому она сопровождается массированной идеологической кампанией, направленной на мифологизацию терроризма.

4. США стремятся придать терроризму статус глобального явления с целью выстроить под своей эгидой международный фронт борьбы, обеспечить военное присутствие в «жизненно важных» регионах мира и сконцентрировать усилия против потенциального противника – «оси зла» (Иран, Ирак, Северная Корея).

Многие исследователи международного терроризма указывают на «сетевую» природу его организации, придающую ему особую «живучесть». Кстати, именно по «принципу паутины» строилась в США глобальная информационная сеть Интернет на случай ядерной войны, чтобы сохранить государственное управление в стране. Государства могут противодействовать сетевым структурам террора лишь системными мерами. Например, устаревшая структура государственного информационного обеспечения создала опасный разрыв в системе национальной безопасности США. ЦРУ не имело права работать внутри страны, а ФБР занималось лишь уголовными преступлениями. В результате они «проглядели» теракты 11 сентября 2001 г. Понадобилось создать новое управление внутренней безопасности, которое закрыло эту

«брешь» между ЦРУ и ФБР, повысило информационно-аналитические возможности государства по раскрытию внутренних террористических угроз. Таким образом, были усилены системные возможности государства по борьбе с терроризмом.

Информационная война террористов отличается от обычной тем, что противник в ней не противостоит открыто. Он анонимен (скрытен) и асимметричен в действиях, применяет информационные средства поражения. Террористы получают потенциальную возможность наносить удары в реальном масштабе времени в кибернетическом (виртуальном) пространстве государства, несоизмеримом с его геополитическим положением. Стратегии боевых действий террористов будут ориентированы на выбор критических точек в системах информационной инфраструктуры, от которых зависит военная мощь или безопасность государства.

Из изложенных рассуждений вытекает ряд методологических оснований для информационного обеспечения борьбы с международным терроризмом.

Во-первых, с международным терроризмом как информационным и политическим по своей природе явлением наиболее эффективными средствами борьбы являются политические и информационные технологии.

Во-вторых, учитывая, что терроризм – это «информационное зло», то необходимо, прежде всего, искать эффективные средства борьбы против него на путях информационного противодействия терроризму.

В-третьих, эффективность информационных средств борьбы многократно возрастет, когда они применяются системно, целенаправленно, оперативно и с упреждением. Решать такой круг специальных антитеррористических задач способна только система информационного обеспечения борьбы против международного терроризма, формированием которой должно озаботиться государство как ее главный субъект.

В-четвертых, такая система информационного обеспечения борьбы с терроризмом может представлять собой интегрированную совокупность сил и средств информационного взаимодействия в обществе, его технологий и организационно-функциональных структур, объединенных общностью целей и задач контртеррористической борьбы, проводимой государством.

В-пятых, система информационного обеспечения требует основательной концептуальной проработки, формирования организационных структур и органов управления, специальных информационных ресурсов, создания подсистем информационной безопасности и противодействия, разработки специальных информационных технологий, налаживания мониторинга террористических угроз и опасностей, контртеррористической подготовки PR-специалистов, совершенствования информационного законодательства государства и т.д.

В-шестых, система информационного обеспечения борьбы против терроризма должна быть сопряжена с другими системами информационного обеспечения жизненно важных сфер деятельности государства (политической, экономической, военной и т.д.). Все это требует проведения более активной национальной информационной политики, в которой также должны быть предусмотрены приоритеты информационной безопасности, увеличивающие контртеррористический потенциал в развитии информационной инфраструктуры и единого информационного пространства общества и государства.

Особую роль в антитеррористической борьбе играет Интернет. Безграничность сети превращает ее не только в инструмент глобализации, своего рода катализатор развития информационного общества, но и в арену террористических действий. Такая специфика Интернета по определению делает его как фактором политической борьбы, так и средством политики государства. Вместе с тем Интернет, фактически превратившись в электронное средство массовой информации, юридически не имеет такого статуса и остается вне поля правовой регламентации, что в целом соответствует общемировой практике. Такая ситуация превращает сеть в мощное и не регулируемое законами средство политической борьбы (например, «сетевая агитация или пропаганда» в период военных действий).

В разработке информационных стратегий борьбы с международным терроризмом могут быть полезны идеи рефлексивного управления. Еще в древнекитайской философии, особенно в даосизме и конфуцианстве, традиционно много внимания уделялось интеллектуально-психологическим способам борьбы с противником. В частности, практика рефлексивного воздействия на врага рассматривалась как неотъемлемая часть политического и военного искусства [3]. Таким образом, роль рефлексивной практики как информационного средства обеспечения борьбы с терроризмом не вызывает сомнения. Это имеет принципиальное значение для разработки моделей стратегии в политике по типу устойчивых интеллектуальных систем, действующих в условиях деструктивных и дестабилизирующих воздействий международного терроризма на систему безопасности государства. Более того, сегодня фактор информационного обеспечения приобретает особую актуальность для военной политики государства в связи с активной разработкой в ряде стран мира стратегий информационно-сетевых войн и войн шестого поколения.

Архитектура систем политики и безопасности России во многом сохраняет еще следы архаичности, характерные для времен холодной войны. Идеологические аргументы нередко преобладают над холодным научным расчетом в политике. Сегодня следует активно искать интеграционные механизмы на основе системы информационного обеспечения, которые связали бы воедино потенциальные возможности, средства и ресурсы государства, необходимые для реализации целей внутренней и внешней политики России, включая эффективное противодействие международному и внутреннему терроризму.

В этой связи можно выделить следующие факторы, влияющие на правовое регулирование в глобальном информационном пространстве и противодействующие терроризму:

1) особенности макроэкономической политики государства;

2) идеология формирования информационного общества;

3) специфика действующего законодательства;

4) особенности менталитета, национально-культурные особенности.

Представляется, что основными направлениями правового обеспечения безопасности глобального информационного пространства будут: 1) определение порядка доступа к информации при гуманном использовании информации; 2) определение доступа к информации в случае использования информации во вред человеку.

Практика показала, что почти бесполезно устанавливать правовой порядок работы по получению и использованию информации через Интернет, ибо ответственность за использование непроверенной и часто недостоверной информации никто не несет, как и за нарушение авторских и смежных прав.

Наиболее эффективным может стать установление ответственности при вводе информации в сети Интернет (установление порядка распространения служебной информации, информация авторского происхождения, официальная и справочная информация).

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. О противодействии терроризму: Федер. закон Рос. Федерации, 6 марта 2006 г., № 35-ФЗ // Собр. зак-ва Рос. Федерации. – 2006. – № 11. – Ст. 1146.

2. Грачева, Т.В. Социальная доминанта в войнах США на рубеже XX–XXI веков / Т.В. Грачева // Безопасность. – 2002. – № 1-2. – С. 64.

3. Китайская наука стратегии. Сер. Каноны / сост. В.В. Малявин. – М.: Белые альвы, 1999.

4. Смолян, Г.Л. Информационное оружие как геополитический инструмент силовой политики / Г.Л. Смолян, Д.С.Черешкин. – М.: ИСАРАН, 1997.

5. Современный словарь иностранных слов. – М.: Рус. яз., 1993. – С. 605.