Евразийский национальный университет им. Л.Н. Гумилева
Факультет журналистики и политологии
Кафедра политологии

МӘҢГІЛІК ЕЛ – ОБЩЕНАЦИОНАЛЬНОЕ ЕДИНСТВО, МИР И СОГЛАСИЕ

Материалы - Международной научно-практической конференции (г. Астана, 2017г.)

УДК 378:327(063)
ББК 74.58+66.4
М 36

Ответственный научный редактор Нечаева Е.Л.
К.п.н., профессор

Редакционная коллегия:
Копежанова Д.Е., Дюсембекова М.К., Жанпеисова Қ.Д.

Мәңгілік Ел – Общенациональное единство, мир и согласие: сбор.матер.VI-Межд. науч.-прак. конф.– Астана, ТОО Мастер По, 2017.- 174 с.

ISBN 978-601-301-928-4

Сборник материалов международной научно-практической конференции содержит доклады ученых, докторантов, магистрантов и студентов казахстанских и зарубежных вузов.

В нем рассматриваются ключевые аспекты социальных и политических процессов Евразийской интеграции, социально-коммуникативные технологии и инновационные процессы в обществе.

В материалах сохранен авторский стиль. Материалы сборника предназначены для широкого круга научной и научно-педагогической общественности, могут быть использованы в теории и практике прикладной политологии и международных отношений.

Ответственность за аутентичность и точность цитат, имен, названий и иных сведений, а также за соблюдение Закона об интеллектуальной собственности несут авторы публикаций и научные руководители.

УДК 378:327(063)
ББК 74.58+66.4

ISBN 978-601-301-928-4

құрдымға жібергенін-де білеміз. Тіршілік тезіне төтеп бере алмай, жер бетінен ұлт ретінде жойылып кеткен елдер қаншама? Біз өзгенің қателігінен, өткеннің тағылымынан сабақ ала білуіміз керек. Ол сабақтың түйіні біреу ғана – «Мәңгілік ел» біздің өзіміздің қолымызда. Ол үшін өзімізді үнемі қамшылап, ұдайы алға ұмтылуымыз керек. Байлығымыз да, бақытымыз да болған мәңгілік тәуелсіздігімізді көздің қарашығындай сақтай білуіміз керек. «Қазақстан 2050» мәңгілік елге бастайтын ең абыройлы, ең мәртебелі жол. Осы жолдан айнымайық, сүйікті халқым! Әрбір күніміз мерекелі, әрбір ісіміз берекелі болсын. Дамуымыз жедел, келешегіміз кемел болсын. Жарқын іспен күллі әлемді таң қылып, Жасай берсін елдігіміз мәңгілік!», - деп Елбасы өз тәуелсіздігімізді сақтау арқылы Мәнгілік ел бола алатынымызды атап, өз Жолдауын аяқтайды. [4]

«Аянбай еңбек ету», «Хақ жолында адал болу», «Жетімдер мен жесірлерді жылатпау», «Зейнеткерлер мен мүгедек жандарға қамқор болу» секілді күнделікті айтып жүрген ұрандарды ақиқатқа, орындалған іске айналдыруымыз тиіс. Міне, сонда ғана «Қазақ Елі Мәңгілік Мұратын» бастап, ұрпағына осы дәстүрді жалғастыруды табыстап отыратыны сөзсіз.

Ең бастысы тәуелсіздігіміз тұрақты, еліміз тыныш, халқымыз аман, бейбітшілігіміз баянды, ұрпағымыз білімді болсын!

Пайдаланылған әдебиеттер тізімі

1. «MANGI EL» халықаралық ғылыми-көпшілік тарихи журналы, — Алматы, «Pride Print», баспасы, 09.2013. — 108 бет.

2. В чем значение формулы «Казахстан - Мәнгілік Ел»? //altyn-orda.kz/v-chemznachenie

3. «Қазақстан жолы – 2050: Бір мақсат, бір мүдде, бір болашақ»

4. ҚР Президенті Н.Ә. Назарбаевтың 2014 жылдың 17 қаңтарындағы Қазақстан халқына кезекті жолдауы

Нуртазин Д.М.
магистрант специальности «Политология»
ЕНУ им. Л.Н. Гумилева
г. Астана, Казахстан
(Научный руководитель: к. полит. н., профессор Нечаева Е.Л.)

РИСКИ, УГРОЗЫ, СОВРЕМЕННЫЕ ТЕНДЕНЦИИ ПОЛИТИЧЕСКОГО ХАКТИВИЗМА И КИБЕРТЕРРОРИЗМА

Об угрозе кибертерроризма и важности развития информационной безопасности в стране, Президент Н.А.Назарбаев отметил в своем послании

народу Казахстана от 31 января 2017 г. “Необходимо проводить работу по предупреждению пропаганды религиозного экстремизма, в том числе в Интернете и социальных сетях[1].

В контексте формирования новых тенденций в мировой политике кибертерроризм и политический хактивизм представляет собой многогранное явление, влияющее на все стороны общественной жизни: политику и экономику, национальные отношения, идеологию и религию.

Актуальность также заключается в том, что за последние годы вопросы, связанные с информационной безопасностью, окончательно перешли в разряд важнейших приоритетов международной безопасности. Свидетельствами этого стали сразу несколько событий и процессов, которые выглядят дистанцированными друг от друга, но уходят корнями в одну и ту же проблематику.

Во-первых, политический кризис на Украине 2013—2014 г. в мировом экспертном, медийном и политическом дискурсе оказалось неразрывно связано с ролью информационно-коммуникационных технологий (ИКТ). Обилие непроверенной информации и попытки манипулирования ей привели к искажению глобальной информационной картины событий, которые происходили на Украине, в том числе территориальные разногласии относительно полуострова Крым. И первые киберстолкновения показывают реальность обозначенной проблемы. Так, в контексте разногласий между Российской Федерацией и США по вопросам смены власти на Украине в 2014 году и референдума жителей Крымского полуострова, на официальные Интернет-ресурсы органов государственной власти, СМИ, крупнейшие бизнес структуры обрушился шквал атак политически ангажированных хакеров - «хактивистов» [2].

Во-вторых, гражданская война в Сирии где примерно за месяц до начала беспорядков в социальной сети Facebook появилась новая группа «Сирийская революция-2011», призывающая ко «Дню гнева» в городах Сирии против президента страны Башара Асада [3]. Беспрецедентная скорость распространения информации через интернет (в основном через социальные сети) сыграла против режимов, стремившихся скрыть свои репрессивные акции от международного сообщества и не владевших адекватными навыками ведения информационной борьбы.

В-третьих, инициативы Казахстана, России и представителей Шанхайской организации сотрудничества, направленные на формирование глобального режима обеспечения безопасности информационного пространства. Речь идет прежде всего о концепции Конвенции ООН «Об обеспечении международной информационной безопасности». Концепция была презентована международному сообществу в ноябре 2011 г. на конференции по киберпространству в Лондоне. Чуть менее резонансной, но столь же масштабной по своим целям инициативой стал проект Правил

поведения в области обеспечения международной информационной безопасности, направленный Генеральному секретарю ООН 12 сентября 2011г. письмом от четырех государств - членов ШОС.

Мировая общественность обратила внимание на хактивизм после событий в Эстонии (в 2007 году) и в Грузии (в 2008 году). Эти две кибератаки, больше напоминавшие начальную стадию кибервойны, чем то, что мы сегодня называем хактивизмом, резко отличались от атак, объектами которых стали противники WikiLeaks и такие компании, как Monsanto. Свои идеи хактивизм черпает из политического активизма, для которого характерен акцент на акциях прямого действия. Многие хактивисты, разделяющие либертарианские идеалы (стремление к сохранению свободы предпринимательства, гражданских свобод, свободы слова и свободы обмена информацией), выступают также в защиту свободы Интернета. Примером акций прямого действия могут служить акции членов «Гринпис», выходящих в открытое море, чтобы помешать ведению китобойного промысла; мирный захват парка в центре Нью-Йорка тысячами активистов по призыву организации Adbusters в рамках «Захвати Уолл-стрит» в июле 2011 года [4]. Добавив к политическому хактивизму сетевую активность хакеров (действующих как с добрыми, так и со злыми намерениями), мы получим хактивизм. 27 сентября 2010 года директор Совета информационных технологий министерства промышленности Ирана Махмуд Лиайи заявил, что атаке подверглось около 30.000 компьютеров. "Компьютерный червь способен передавать информацию о производственных процессах и ходе разработок за границу нашим врагам. Ирану объявили электронную войну", - провозгласил Лийаи [5].

Опираясь на труды исследователей кибертерроризма, на современном этапе функционирования кибертерроризма как явления, угрожающего национальной безопасности государства, можно выявить следующие тенденции его развития:

1. Неуклонный рост создаваемой им общественной опасности, который выражается в том, что общий уровень проявления экстремизма и терроризма, как в Республике Казахстан, так и во всем мире, постоянно возрастает. Также необходимо отметить, что современные достижения научно-технического прогресса увеличивают вероятность применения изначально мирных технологий в качестве средств проведения кибератак, причём подобное их использование во вред порой даже не осознаётся создателями этих технологий;

2. Расширение масштабов воздействия на различные социальные слои. Эта тенденция проявляется в использовании кибертеррористами информационно-коммуникационных сетей и систем, посредством которых происходит воздействие на большие массы людей (например, социальные сети), при слабой цензуре или полном отсутствии какого-либо контроля со

стороны государства, а также в быстром и относительно дешёвом распространении информации;

3. Возрастание изощрённости и антигуманности кибертеррористических актов обусловлено тем, что на сегодняшний день у кибертеррористов есть реальная возможность нарушить нормальное функционирование критически важных объектов государства (ядерные реакторы, биологические и химические лаборатории и т. д.), что может повлечь за собой неисчислимое количество жертв;

4.Политизация кибертерроризма, проявляющаяся в стремлении кибертеррористов влиять на принятие государственных решений в целях ослабления деятельности правоохранительных органов, торможения законодательных инициатив посредством насильственных методов (кражи или уничтожения информации, шантажа, угроз, порчи компьютеров);

5. Улучшение технической оснащённости кибертеррористов. Кибертерроризм относится к технологическим видам терроризма. В отличие от традиционного, этот вид терроризма использует в террористических акциях новейшие достижения науки и техники в области компьютерных и информационных технологий, радиоэлектроники;

Методы, посредством которых Интернет используется в террористических целях. Для целей настоящей публикации в отношении классификации методов, посредством которых Интернет нередко используется для поощрения и поддержки террористических актов, был принят функциональный подход. На основе такого подхода были определены частично перекрывающих друг друга категорий: пропаганда (в том числе вербовка, радикализация); финансирование; исполнение; а также компьютерные атаки. Каждая из этих категорий более подробно рассматривается ниже.

Пропаганда. Одним из основных направлений использования Интернета террористами является пропагандистская деятельность. Обычно пропагандистские материалы имеют форму мультимедийных коммуникаций, содержащих идеологические или практические наставления, разъяснения, оправдания или рекламу террористической деятельности. К ним могут относиться виртуальные сообщения, презентации, журналы, теоретические работы, аудио- и видеофайлы, а также электронные игры, разрабатываемые террористическими организациями или их сторонниками. Пропаганда экстремистской риторики с призывами к насильственным действиям также является общей тенденцией для все более широкого круга интернет-платформ, предоставляющих услуги по размещению информационного наполнения, создаваемого пользователями. Материалы, которые прежде могли распространяться – лично или с помощью физических носителей, таких как компакт-диски (CD) и цифровые видеодиски (DVD), – среди относительно ограниченной аудитории, все чаще переносятся в Интернет. Основная угроза,

которую несет с собой террористическая пропаганда, связана с тем, как она используется и в каких целях распространяется. Распространяемая через Интернет террористическая пропаганда охватывает ряд задач и аудиторий. Она может быть приспособлена для воздействия, в частности, на потенциальных или реальных сторонников, или противников той или иной организации или общих экстремистских воззрений, на прямых или косвенных жертв террористических актов или на международное сообщество в целом либо какую-то его часть.

Вербовка. Интернет может использоваться не только в качестве средства для публикации экстремистской риторики и видеоматериалов, но и как способ установления отношений с теми, кто наиболее склонен поддаваться на целенаправленную пропаганду, и поиска их поддержки. Террористические организации все чаще используют пропаганду, распространяемую через такие платформы, как защищенные паролем веб-сайты и чат-группы ограниченного доступа в Интернете, как средство тайной вербовки. Совокупная аудитория Интернета обеспечивает террористическим организациям и их сторонникам глобальный резерв потенциальных новобранцев. Интернет-форумы ограниченного доступа становятся для новообращенных тем местом, где они могут узнать о террористических организациях и предложить им свою поддержку, а также приступить к непосредственным действиям, чтобы способствовать террористическим целям. Использование технологических барьеров для доступа к платформам, на которых осуществляется вербовка, кроме того, усложняет процесс отслеживания сотрудниками разведки и правоохранительных органов связанной с терроризмом деятельности.

Радикализация. Относится прежде всего к процессу идеологической обработки, который нередко сопутствует превращению завербованных неофитов в лиц, преисполненных решимости совершать насильственные действия на основе экстремистских идеологий. Процесс радикализации часто включает использование пропаганды, которая на протяжении длительного времени ведется либо посредством личного общения, либо через Интернет. Продолжительность и эффективность пропаганды.

Финансирование. Террористические организации и их сторонники также могут использовать Интернет для финансирования террористических актов. Методы, с помощью которых террористы используют Интернет для мобилизации и сбора средств и ресурсов, можно подразделить на четыре основные категории: прямые просьбы о пожертвованиях, электронная коммерция, использование действующих в Интернете платежных инструментов, а также посредничество благотворительных организаций. В случае прямых обращений речь идет об использовании веб-сайтов, чат-групп, массовых рассылок и целенаправленных сообщений в целях передачи просьб о пожертвованиях от сторонников. Веб-сайты также могут использоваться в качестве интернет-магазинов, предлагающих сторонникам книги, аудио- и

видеозаписи, и другие товары. Платежные средства, предоставляемые в Интернете через специализированные вебсайты или коммуникационные платформы, позволяют легко осуществлять электронный перевод средств между сторонами. Переводы средств нередко производятся с помощью электронных банковских переводов, кредитных карт или иных платежных средств, доступных через такие сервисы, как PayPal или Skype.

Рассматривая угрозы информационной безопасности как факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве, предполагается наличие следующих направлений, по которым возможны проявление этих факторов:

1. Противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны. Такое противоборство обозначено категорией «информационная воина».

2. Использование информационных ресурсов или воздействие на них в информационном пространстве в противоправных целях. Терминологически это направление обозначено как «информационная преступность».

3. Использование информационных ресурсов или воздействие на них в информационном пространстве в террористических целях. Обозначается как «кибертерроризм».

Основной формой кибертерроризма является информационная атака на компьютерную информацию, вычислительные системы, аппаратуру передачи данных, иные составляющие информационной инфраструктуры, совершаемая группировками или отдельными лицами. Такая атака позволяет проникать в атакуемую систему, перехватывать управление или подавлять средства сетевого информационного обмена, осуществлять иные деструктивные воздействия.

Информационные технологии широко используются террористическими организациями для пропаганды своей деятельности, а также для вовлечения в нее новых членов. В настоящее время в Интернете находятся сайты практически всех более или менее крупных исламистских организаций, в том числе радикального толка («Исламский джихад Палестины», «Хезболлах» и др.). Большинство таких сайтов образуют специфическую подсеть в Интернете, главные цели которой – это информационно-пропагандистское воздействие и организационная деятельность. Кроме того, Интернет используется радикальными группировками в качестве средства связи. Так, по утверждению специалистов из израильской контрразведки Шин-Бет, «террористы» передают через электронную почту в зашифрованном виде инструкции, карты, схемы, пароли и т.д [6 с.129]. Довольно активно возможности сети Интернет используют и различного рода прочеченские

организации экстремистского направления. По сообщениям СМИ, в ряде стран ближнего зарубежья продолжают действовать информационные центры террористов, занимающиеся тенденциозным подбором информации о ситуации на Северном Кавказе в целях манипулирования международным общественным мнением, в Интернете находится ряд сайтов, связанных с таким центром и размещающих подготовленную им информацию.

Как уже отмечалось, новые информационные технологии предоставили террористам совершенно новые, угрожающего масштаба возможности воздействия на безопасность личности и общества. В связи с этим в области обеспечения безопасности появилось новое понятие «информационное оружие» – создание и использование информационно-коммуникационных технологий с целью нарушения работоспособности информационных систем и информационно-коммуникационных сетей критически важных объектов инфраструктуры общества и государства. Киберпространство привлекает террористов, так как, по мнению специалистов, Интернет позволяет группе или индивиду казаться более значительным или угрожающим, чем они есть на самом деле. При обеспечении безопасности киберпространства необходимо учитывать целый ряд его специфических особенностей, позволяющих группе или индивиду продвигать их идеи. Эти особенности, являясь сами по себе нейтральными или даже содержащими множество позитивных возможностей, в руках террористов становятся чрезвычайно опасными. В числе таких особенностей анонимность, конфиденциальность, доступность, низкая стоимость, легкость в использовании, внимание масс-медиа, психологическое воздействие.

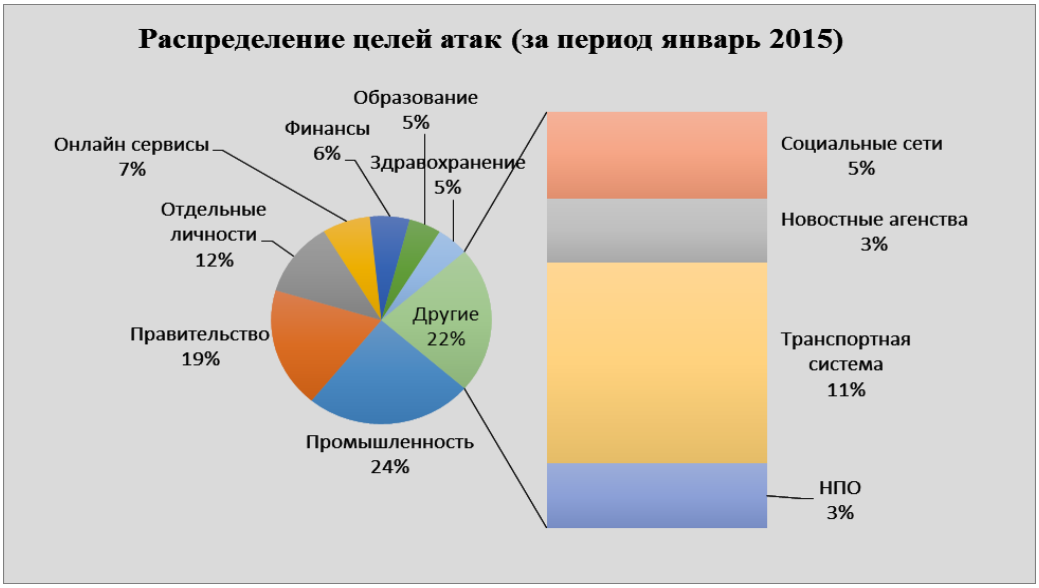
Конфиденциальность и доступность приемов кодирования облегчает взаимодействие для террористических организаций. Возрастающее присут-ствие оцифрованных медиа и алгоритмов шифровок позволяет террористам общаться через секретные электронные каналы. Более того, коммуникацию террористов сложно обнаружить, когда они пользуются электронной почтой, так как информация может быть анонимной и данные закодированными. В дополнение к этому террористы могут использовать передовые средства шифровки, такие, как «стеганография» (метод засекречивания сообщения в изображении), чтобы общаться засекречено, используя вебсайты “electronic dead drops” как вложенные в изображения сообщения. Террористы продолжают искать новые методы, позволяющие им общаться тайно.

Всемирное распространение интернет-технологий облегчило доступ к общению через любые границы. Интернет позволяет общаться 24 часа в день с человеком, находящимся в любом уголке мира. И хотя это чрезвычайно удобно в производственных, гражданских и международных целях, подобные технологии позволяют террористам расширить свою коммуникацию и повысить продуктивность взаимодействия.

В соответствии с этим, подобно формам физического терроризма, кибертерроризм – это форма психологической угрозы, призванная вселить страх в

«целевую группу» [7] Терроризм использует киберпространство для распространения пропаганды, изображений насилия, угроз и порождает киберстрах – страх перед лицом возрастающей угрозы кибертерроризма. Террористические группы, такие, как АльКаеда, используют кибер-пространство не только чтобы получить поддержку, но, и чтобы посеять страх среди населения [8].

Учитывая то, что киберпространство выступает как усилитель воздействия, посеять через него страх у населения становится легковы-полнимой задачей: распространение угрозы даже без предъявления плана ее выполнения оказывается достаточным для беспокойства.



Следует отдельно выделить влияние экстремистских организации на молодежь через Интернет. Необходимо отметить, что об этом говорили на республиканской конференции «Новые подходы в информационной работе по противодействию религиозному экстремизму», проходившая 25 декабря 2014 г. в Астане [9]. В ней приняли участие представители Администрации Президента, центральных государственных и местных исполнительных органов, неправительственных организаций, эксперты. В числе участников были журналисты газет «Приуралье» и «Орал өңірі».

В Казахстане проживают около 130 этносов, относящихся к 18 различным конфессиям, самым многочисленным из которых является ислам – более 70% от общего числа верующих и различные направления христианства, в основном, православие – 26%. Согласно статистическим данным центра по изучению проблем терроризма и экстремизма, в Казахстане 73% интересующихся религией граждан пользуются Интернет-сайтами.

Исходя из этого, можно резюмировать, что система противодействию кибертерроризму и политическому хактивизму в настоящий момент находится на

стадии своего развития. Безусловно, говоря о формировании в Казахстане механизмов эффективного сотрудничества, следует прилагать еще более активные усилия для увеличения эффективности и результативности переговорного процесса. Учитывая сегодняшние реалии, а также геополитическую ситуацию в регионе, где пересекаются стратегические интересы крупных стран – необходимо развитие информационной и кибербезопасности в Казахстане.

Список литературы:

1. Назарбаев Н.А Заседание Совета Безопасности 24 февраля 2015. http://www.akorda.kz/ru/events/akorda_news/meetings_and_sittings/page_219208_zasedanie-soveta-bezopasnosti-pod-predsedatelstvom-glavy-gosudarstva.
2. Активисты в Сирии призывают к "пятнице гнева. "http://www.bbc.com/russian/international/2011/04/110428_syria_friday_of_rage_call;
3. Панарин И.Н, Лекция «Актуальные проблемы обеспечения информационной безопасности Евразии 2014 г».
4. Махмутов А. Концепция национальной безопасности Казахстана в контексте современных внешнеполитических процессов 2015 г.
5. Акопов Г.Л. Информационное право в контексте современных тенденций. http://www.ozon.ru/context/detail/id/4041940/.
6. Дмитриенко Т.А. Обеспечение информационной безопасности и развитие информационной инфраструктуры Республики Казахстан // Информационно-аналитический журнал «ANALYTIC». — 2003. — № 5. — С. 12-14.
7. Карин Е.Т Статья «У нас нет иммунитета к информационным вирусам». http://www.ozon.ru/context/detail/id/4041940/.
8. Стрельцова А.А. Актуальные проблемы обеспечения информационной безопасности // Технологии безопасности. № 11. С. 54.
9. Уильям Тафойа Cyber Terror. https://leb.fbi.gov/2011/november/cyber-terror.
10. Джэйсон Сэк 1999. How Terrorism Ends. US Institute of Peace working group report, May 1999. 11.Collin, B., 1997. The Future of Cyberterrorism, Crime and Justice International, March 1997, pp.15-18.

М.Ю. Онучко
к.полит.н., профессор кафедры политологии
ЕНУ им. Л.Н.Гумилева
г. Астана, Казахстан

ЗАРУБЕЖНЫЙ ОПЫТ ПРОТИВОДЕЙСТВИЯ И ПРОФИЛАКТИКА ТЕРРОРИЗМА

С момента появления первых террористических атак, на взгляд автора дипломного проекта человество предпринимало шаги и пути по противодействию терроризму.