Гуманитарные и социально-экономические исследования в новой парадигме научного знания

УДК 304
https://doi.org/10.36906/KSP-2021/01

Аймухамбетов Т.Т.
ORCID: 0000-0001-5345-6843, доктор Ph.D.
Калемшарив Б.
Евразийский Национальный университет имени Л.Н. Гумилёва
г. Нур-Султан, Казахстан

ДЕСТРУКТИВНОЕ ВЛИЯНИЕ В ИНТЕРНЕТЕ ЭКСТРЕМИСТСКИХ ОРГАНИЗАЦИЙ

Аннотация. Современный процесс глобализации делает современные опасности более актуальными, в особенности, такие, как вооружённый конфликт, распространение вирусов и инфекций, проблема с экологией или деструктивная деятельность организованных криминальных банд. Та как глобальная сеть и новые технологии не только делают нашу жизнь легче и лучше, но при этом таят в себе опасность, приводящую к появлению новых угроз в рамках международного сообщества, которая станет фатальной для него. Например, использование преимуществ глобальной сети для свержения «неугодных политических режимов» приведёт к росту социальной напряженности и созданию благоприятной почвы для деятельности экстремистских организаций.

Ключевые слова: Интернет; религия; экстремизм; деструктивное влияние; общество.

Aimukhambetov T.T.
ORCID: 0000-0001-5345-6843, Ph.D.
Kalemsharif B.
L.N. Gumilyov Eurasian National University
Nur-Sultan, Kazakhstan

THE DESTRUCTIVE INFLUENCE OF EXTREMIST ORGANISATIONS ON THE INTERNET

Abstract. The current process of globalisation is making contemporary threats more acute, in particular armed conflict, the spread of viruses and infections, environmental problems or destructive activities of organised criminal gangs. The global network and new technology will

not only make our life easier and better, but will also pose fatal threats to the international community. For instance, using advantages of the global network to overthrow «undesirable political regimes» will lead to growing social tensions and create a fertile ground for activities of extremist organizations.

Key words: Internet; religion; extremism; destructive influence; society.

Мировое сообщество находится на переходе на новую ступень развития, и активное развитие новых технологий яркое тому доказательство. В данном направлении угрозой для этого развития может стать: активное использование средств новых технологий в деструктивной деятельности экстремистских организаций и групп.

Рост радикализма, экстремистская деятельность и деструктивные действия – реальная угроза невзирая на посильные меры международного сообщества в борьбе с данной угрозой.

Первостепенной угрозой в данном направлении являются деструктивные действия (террористический акт), который до определённого момента имел точечный и анонимный характер. Так по данным исследования университета Мэрилин, начиная со второй половины XX века происходит рост деструктивной активности по всему мировому сообществу [6, с. 19]. Кроме того, происходит рост жертв от данных действий, например, 2012 год отмечен как год активной деструктивной деятельности, когда погибло от этого около 16 тысяч человек (https://clck.ru/ZCX94). Данные события являются проблемой всего мирового сообщества, так как опыт показывает, что его проявление не зависит от уровня развития, религиозной направленности и географического расположения, перед этой угрозой все равны.

Вторым немаловажным фактором является «информационная война», по которой пока нет единного понимания ее сущности. Данный факт направлен на большие категории потребителей, а не единичный формат воздействия. Их можно сравнить с методикой психотерапии, влияя на индивидуальное сознание ты воздействуешь на массы. Орудием в данной войне являются все средства передачи информации. Данное воздействие имеет в себе выгодная интерпретация событий, изменение эмоционального восприятия данных событий и все в выгодную позицию управляющей стороне. Например такая комбинация не нова и часто использовалась в истории человечества:

Чингисхан намеренно сгущал краски по поводу их набегов, что постепенно снижало боевой и моральный дух следующих потенциальных противников;

Ведь неспроста философ Древней Греции утверждал, что для сокрушения кого либо, первоначально надо сокрушить его сознание. Соответственно можно прийти к выводу, что данное направление существовало достаточно давно в историческом процессе развития человечества [7, с. 147].

Ниже процитируем представителя вооружённых сил США генерала Джона Рэймонда, определившего следующий тезис: «Цель информационной войны – повлиять на поведение соперника, без сознания это им. Успех в данном направлении заключается в моральной дезориентировке соперника. Также целью является создания преград для проведения

скоординированных и эффективных действий. Это помогает добиться наших целей и помешать добиться этих целей сопернику» (https://clck.ru/ZCXef). Исходя из выше анализированного, можно с уверенностью определить, что экстремистская деятельность - это дестабилизация институтов общественной деятельности при минимальных затратах ресурсов. С этим согласны аналитики США в области экстремизма Дуглас Джонсон и Джон Мартин, утвердившие немыслимость существование современного террора без медиа фактора (https://clck.ru/9SD65). Акт терроризма, может вызвать дестабилизацию общества, при этом средства массовой информации будут только нагнетать обстановку. В конце концов в процессе активизации радикализации мирового сообщества, произошла модификация методик воздействия на идейном уровне соответствующих групп, для повышения уровня новых адептов и качественный подъем деструктивной деятельности в информационной сфере. Это объяснимо тем, что радикальное действие является одновременно – мощное информационное оружие, действие которого приносит намного больше вреда чем сам террористический акт. Соответственно можно прийти к выводу, что возможности глобальной сети и современных технологий делают деятельность экстремистских организаций намного проще. Эти средства становятся основным дестабилизирующим методом воздействия на молодое поколение. Так 28.10.2010 в ходе 65-й сессии Генеральной Ассамблеи ООН была принята Резолюция, где был поднят вопрос о угрозе в информационной среде. В особенности наглядным было, что в данном контексте особую угрозу определили именно информационную глобальную сеть – Интернет, что в некоторой степени дало относительную свободу государственным образованиям по регулированию данного направления (https://clck.ru/ZCYMK).

Произведённый анализ показал три способа деструктивного действия экстремистских организаций с использованием глобальной сети, что отражено в таблице:

Таблица

Вид угрозы	Последствия
Хакерская атака на сеть	Приводит к дестабилизации системы, что приводит к повышению социальной напряженности
Массовая рассылка опасной информации	Вербовка новых адептов, дестабилизация общественного сознания.
Сбор личной информации для шантажа	Точечный удар для поиска объектов для деструктивных действий.

Из данного направления появился термин «Кибертерроризм», введённый Барри Коллином. Данным термином он пытался поднять вопрос о переходе экстремистской деятельности из мира реального в мир виртуальный. Но при этом это не определяет более чётко данное выражение. Кибертерроризм означает – атаку на стратегические информационные системы общества, целью которой является дестабилизация социально-экономической жизни страны, коллапс экономического развития, сделать регион более подверженным внешнему нападению [2].

Сама природа Кибертерроризма акцентировала создание целенаправленно организаций с узкой идеологической платформой, например – «Электронный Джихад». Данная организация неформально поддерживается некоторыми странами Ближнего Востока со времени его появления, а именно в 2009 году [5]. Уникальность данного направления в том, что методика их заключалась в парализации основных аспектов жизнедеятельности, начиная от социально-экономической, заканчивая проблемами обороны определённых государственных образований. Таким образом сам «Джихад» смог перейти от реального воздействия к деструктивной деятельности в виртуальном мире, последствия которого стали намного больше предыдущего.

В электронных системах, связанных с данным направлением организаций, производится набор для деятельности в глобальной сети в интересах данных движений и организаций. Пример заключён в следующем: В 2000 году после срыва мирных договоров между государством Израиль и Палестинской автономией, хакеры данных стран провели ряд атак, что в некоторой степени парализовало некоторые сферы общественной деятельности, что побудило к росту физического насилия в регионе (https://clck.ru/ZCZ4s). Суть «Электронного Джихада» в активной информационной атаке на основные аспекты жизнедеятельности для набора новых адептов и увеличению своего влияния на внутриполитические процессы в данном регионе или стране.

Непосредственным объектом Кибертеррористов стали компьютерные игры. Например, такие игры, как “Strike Force”, “Shootem up” создают героический образ экстремиста и образ врага – представителей органов правопорядка, что бессознательно влияет на самосознание молодого поколения. Данной методикой пользуются достаточно много экстремистских организаций, в том числе до определённого момента «ИГИЛ» (https://clck.ru/ZCZNB).

Распространяя о себе в таком контексте, данные организации становятся ближе к молодому поколению, беседуя на понятном им языке [4, с. 56].

В последнее время наблюдается рост идеологического воздействия через глобальную сеть, не имеющую границ. Примером может послужить анализ найденных информационных каналов данных организаций в глобальной сети. Данный анализ произведён в виде диаграммы, которая будет опубликована ниже (рис.). В данной диаграмме будет отмечен рост количества экстремистских организаций в глобальной сети Интернет:

Рис. Количество веб-сайтов экстремистских организаций в Интернете с 2000 по 2020 гг. по данным Центра исследования проблем религий города Нур-Султан

Данная тенденция показывает о стремлении радикально религиозных групп и организаций заполонить основные постулаты сети своим информационным контентом [4]. В этом плане борьба усложняется самим фактом существования информационных потоков, не доступных поисковым системам. Данные контенты обычно называют «серым интернетом», и обычно выступают под никами: “Dark Net”, “Deep Net”, “Free Net”. Данная сущность делает глобальную сеть благоприятной почвой для экстремистских организаций, для совершения ими деструктивных действий, без последующей возможности поймать их [1, с. 104].

Из всех систем в глобальной сети, наибольшей популярностью у них пользуется почтовая система. Лёгкость, простота и дешевизна распространения информация, плюс если помещается информация в облако и открывается к нему доступ, можно и не попасться в проведении агитации экстремистских организаций. Так поступала «Аль-Каида», для мобильной связи со своими адептами. Есть информация, что террористы, совершившие теракт 11.09.2011 г., использовали стандартные почтовые программы для связи с друг другом и своим руководством (https://clck.ru/ZCZTa).

Также популярным методом экстремистских организаций являлось использование хэштэгов для деструктивной деятельности в идеологическом контексте против развитых стран Запада. Например, “#BostonBombings” – хэштэг, намекающий на участие данных организаций в террористическом акте в Бостоне США в 2013 году [1, с. 56].

Также немаловажным методом является программа Ask.fm, где игра слов при ответах на вопросы, люди затягиваются идеей проведения Джихада и бессознательно становятся адептами данных организаций. Одно время это было опасной угрозой в странах Центральной и Восточной Европы, ввиду популяризации данной программы в определённый период (https://clck.ru/ZCZVn).

Исходя из этого, информационные каналы могут спокойно стать центрами для подготовки новых адептов. Экстремисты для этого работают через скрытые каналы, прикрывающиеся безобидными темами общего религиозного значения. Активным использованием вербовочных технологий пользуются высококвалифицированные представители, использующие манипулятивные методы психологии. Для достижения эффективности в процессе использования проходят различные системы информационного обеспечения общества. Например организация «ИГИЛ» имела в наличии собственный канал, который систематически просматривали около половины миллиона зрителей. Данный канал показывает своеобразные отчёты их деструктивной деятельности, проводят агитационную работу по поиску новых адептов и показывают погоду на ближайшие дни [3]. Данная работа – обычное действие, чьей целью является проведение агитационной деятельности для привода новых адептов в движение.

Литература

1. Адамов А. Технические, юридические и политические вопросы борьбы с терроризмом в Интернет // Терроризм и интернет: Материалы Международной научно-практической конференции (Астана, 25 ноября 2014 года). Астана, 2014. 162 с.

2. Бураева Л.А. Кибертерроризм как новая и наиболее опасная форма терроризма // Проблемы экономики и юридической практики. 2017. № 2. С. 188-191.

3. Джереми Т. Распространённая актуальность: Терроризм и Интернет сегодня // Материалы Международной научно-практической конференции. Астана, 2014. 162 с.

4. Джереми Т. Терроризм и Интернет сегодня // Терроризм и интернет: Материалы Международной научно-практической конференции (Астана, 25 ноября 2014 года). Астана, 2014. 162 с.

5. Мазуров В.А. Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУР. 2010. № 1-1 (21).

6. Онучко М. Терроризм и информационная война: некоторые аспекты проблемы // Терроризм и интернет: Материалы Международной научно-практической конференции (Астана, 25 ноября 2014 года). Астана, 2014. 162 с.

7. Турсынбекова С. О роли органов прокуратуры в противодействии терроризму в интернет-пространстве // Терроризм и интернет: Материалы Международной научно-практической конференции (Астана, 25 ноября 2014 года). Астана, 2014. 162 с.