



Наряду с наземной, морской и воздушно-космической сферами информационное пространство сегодня превратилось в полноценную среду военного противоборства. Приемы и способы боевых операций в нем – это дезинформация, распространение слухов, военная пропаганда, известные со времен античности. Однако лишь с развитием современных информационно-коммуникационных технологий (ИКТ) разрушительность этого средства борьбы достигла качественно нового уровня, сопоставимого с оружием массового поражения. Четкое понимание опасности подобного оружия особенно важно в нынешних условиях жесткой конкуренции между Россией и так называемым коллективным Западом во главе с США .

Под информационным соусом

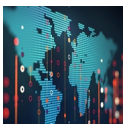


Информационное противостояние не прекращалось с начала холодной войны в 1946 году и вошло в новую, особенно острую фазу весной 2014 года, после возвращения в состав нашей страны Крыма и начала гражданской войны на юго-востоке Украины. Основной его формой наряду с политико-дипломатическим давлением и экономическими санкциями стала полномасштабная информационная война, направленная на подрыв духовного потенциала Российского государства, а также морально-психологического состояния общества и каждой отдельно взятой личности.

В ней активно используется весь потенциал современных ИКТ. В первую очередь средства обработки, отображения и передачи информации. Пионерами их внедрения являются транснациональные, а по сути американские ИТ-корпорации.

Противоборство ведется в условиях глобального доминирования корпоративных СМИ, перешедших в онлайн-формат с сохранением традиционных форм подачи информации, а также возникновения новых площадок – социальных сетей, видеохостингов, интернет-изданий, блогплатформ, подконтрольных крупному американскому бизнесу.

Сама сеть Интернет рассматривается Вашингтоном как главный инструмент гибридной войны для достижения глобального доминирования в мировом информационном пространстве. Более того, США раньше других государств стали рассматривать интернет-технологии как неотъемлемую часть военного потенциала, причем имеющую наступательный характер.



Интернет-диверсанты

С 1994 года под патронатом Пентагона функционирует «Горный форум» (The Highlands Forum) – неформальный «мозговой центр», выступающий в качестве площадки для обмена мнениями наиболее компетентных экспертов в области информационных технологий (за 27 лет проведено 16 общих и 7 специальных собраний). Он финансируется Министерством обороны и работает под председательством замминистра обороны по разведке, курирующего Агентство национальной безопасности

и Разведывательное управление Министерства обороны США.

«Горный форум» – это диалоговая площадка ИТ-компаний, представителей СМИ и руководства военной разведки, где устанавливаются долгосрочные корпоративные связи, выявляются возможности для тонкой настройки стратегии информационной войны в условиях абсолютной секретности. Общее число участников мероприятий – свыше тысячи человек.

“Примечательно, что обвинения в кибератаках зачастую выдвигаются после громких внешнеполитических инициатив Российской Федерации”

«Горный форум» представляет собой неформальную междисциплинарную сетевую структуру, созданную для изучения проблем дезинформации и противоборства в информационной сфере. Решения и рекомендации, принятые его участниками, а также подготовленные аналитические материалы напрямую передаются высшему военному руководству США в строго закрытом режиме.

Главной задачей данного мероприятия является обеспечение американского доминирования в сфере информационного оружия. Наряду с этим оно служит, с одной стороны, для влияния теневой сети подрядчиков на формирование политики информационных операций, с другой – для воздействия военных на гражданский сектор.

Выработанные на платформе «Горного форума» подходы к распространению дезинформации и пропаганды наряду с методами современной журналистики (ведение блогов, создание медиаконтента, стриминг) Запад в полной мере задействует в целях ослабления России. При этом главной фокусной аудиторией является молодежь.

Во-первых, среди нее традиционно популярны нигилистические настроения, во-вторых, люди до 30 лет основным источником получения информации рассматривают именно Интернет. Каналы YouTube и Телеграм, блоги популярных авторов служат для них альтернативой телевидению, радио и печатным СМИ. Через онлайн-площадки продвигаются подрывные идеологические концепции – политического и религиозного экстремизма, а также радикального либерализма, приводящего к эрозии

государственных институтов и духовно-нравственных устоев общества. Размещаемые на них фото и текстовые сообщения наглядны, интерактивны, динамичны. Именно в схожести таких материалов с развлекательно-познавательным продуктом заключается их опасность.



«Российские хакеры»

Деструктивные идеологические концепции, продвигаемые западной пропагандой в российском обществе, можно разделить на две основные группы – общественно-политическую и религиозную. К первой относятся региональный и национальный сепаратизм, радикальный либерализм, прививаемый всегда в комплекте с крайним западничеством и глубоким комплексом национальной неполноценности, пересмотр прошлого России вплоть до его полного переписывания.

Фальсификация истории – отдельное направление идеологической войны против нашего государства и общества. Она ведется на ряде направлений: тиражировании и закреплении стереотипов, исторических мифов о российском менталитете, фрагментации единой истории России на отдельные истории социальных и этнических групп с преобладанием радикально-националистической и русофобской риторики, «переосмыслении» Великой Отечественной войны 1941–1945 годов и подвига советского народа.

К религиозной группе деструктивных идеологических концепций можно отнести радикальный ислам (ваххабизм), псевдохристианские учения (пятидесятничество, свидетели Иеговы, Церковь Иисуса Христа Святых последних дней (мормоны), Церковь объединения (муниты), Церковь Христа, неоязычество и прочее, часто продвигаемое в рамках навязывания национал-сепаратистских идей.

С целью ведения подрывной идеологической войны против Российской Федерации создана специальная инфраструктура НАТО – центры стратегической пропаганды в Польше и странах Балтии. На них возложены задачи постоянного мониторинга социально-политической и информационной обстановки на территории РФ, координации информационных операций в зоне ответственности, а также, что является

главным направлением работы данных органов, поиска и вербовки российских граждан, готовых вести антигосударственную пропагандистскую работу в электронных СМИ и социальных сетях.

Эти структуры являются учебными центрами, где готовят кадры для ведения масштабной долговременной скоординированной информационной кампании, направленной на углубление внутренних противоречий, разжигание ненависти к различным представителям общества, подрыв доверия населения России к государственным структурам.

Для осуществления поставленных целей военно-политическое руководство западных стран применяет комплексный подход, объединяя образование, технологии массовых манипуляций и пропаганды, новейшие достижения общественных наук.

Главными органами НАТО здесь является ряд организаций, в частности:

- Центр передового опыта в области стратегических коммуникаций (Рига, Латвия);
- Центральная группа психологических действий сил специальных операций вооруженных сил Польши (Быдгощ);
- Центр передового опыта НАТО в области киберзащиты (Таллин, Эстония).

Представители западных спецслужб и электронных СМИ, прошедшие обучение в таких центрах, в последние годы активно задействуют методики поиска «цифровых улик» в рамках сфабрикованных обвинений властей РФ и российских спецслужб в нарушении различных международных норм, вмешательствах в дела других государств. Указанную методику также интенсивно использует группа «Беллингкэт», тесно связанная с британской разведкой.

Кампания против российских спецслужб, начатая западными массмедиа, подхваченная русскоязычными либеральными ресурсами и длившаяся на протяжении нескольких лет, стала одной из наиболее масштабных и агрессивных информационных атак против РФ. Именно в ходе нее родился мем «русские хакеры», они же «хакеры ГРУ».

Целью информационной кампании была и остается дискредитация России на международной арене, создание у населения зарубежных стран образа врага – страны-агрессора, страны-кибертеррориста, для чего используются все возможные информационные каналы, существующие традиционные и цифровые медиа, применяются последние достижения ИКТ.

Обвинение Москвы в агрессивной внешней политике – беспроблемная тема для Запада, который ищет новые информационные поводы для диффамации России на геополитической арене. В последнее время к ним добавился еще и универсальный тезис о причастности «русских хакеров» к любым значимым киберинцидентам. Так, член-корреспондент Академии военных наук Сергей Судаков отметил, что на смену «русской мафии» теперь пришли «русские хакеры», которыми пугают население США и Европы.

В ходе информационной кампании против российских спецслужб Запад отработывает один и тот же сценарий, возлагая вину за каждый резонансный киберинцидент на «русских хакеров». В качестве примера подобных огульных обвинений можно привести заявления об атаках на 200 американских НКО и информационные системы органов власти США в сентябре-октябре 2020 года якобы с целью повлиять на предстоящие президентские выборы, взлом электронных почтовых ящиков членов парламента Норвегии.

Весной 2020-го Россия была обвинена в организации кибератак на медучреждения Чехии (март-апрель), британскую медицинскую научно-исследовательскую компанию Hammersmith Medicines Research (март) и университеты, занимающиеся разработкой вакцины против коронавируса (май). Во всех случаях никаких объективных доказательств причастности российской стороны приведено не было.

Примечательно, что обвинения в кибератаках зачастую выдвигаются после громких внешнеполитических инициатив Российской Федерации или на фоне позитивных сдвигов в проблемных отношениях с какими-либо государствами. Например, когда министр иностранных дел Польши Яцек Чапутович 9 мая 2019 года высказался о необходимости «вести конструктивный диалог» с Москвой, сразу последовала информация о причастности «русских хакеров» к рассылке в польские школы электронных писем о минировании.

Под ложным флагом

По такой же схеме Запад действовал и после того, как президент РФ Владимир Путин 22 октября 2020 года озвучил инициативу о введении ограничений на использование киберпространства в рамках вооруженной борьбы. Практически одновременно Министерство юстиции США предъявило бездоказательные обвинения шестерым россиянам во взломе электронных ресурсов предвыборного штаба Макрона (май 2017 года), массовом распространении вируса Not Petya (июнь 2017 года), атаке на оргкомитет зимних Олимпийских игр в Пхенчхане (февраль 2018 года).

Подобная провокация была реализована, повторим, в разгар предвыборной гонки 2020 года в США. В середине сентября – почти за два месяца до общенациональных выборов – директор ФБР заявил о факте вмешательства в них России. Тем самым был создан «формальный повод для обвинений» в отношении РФ, когда любой киберинцидент – реальный, инсценированный либо выдуманный – можно приписать «российским хакерам» и ввести новый пакет санкций в отношении Москвы.

При этом активно отрабатываются методики фальсификации «цифровых следов» – умышленной подмены государственной принадлежности источника атаки и создания искусственных улик для дискредитации России. На языке западных спецслужб это называется false flag operations – операции под ложным флагом.

Для грамотных ИТ-специалистов не представляет труда замаскировать под любую национальную принадлежность почерк работы хакеров – так называемый TTPs (Tactics, Techniques and Procedures – тактика, методы и технологии). А с целью поддержания химеры русского следа нанимаются русскоязычные программисты из Украины и стран Балтии, которые целенаправленно вносят русизмы в программные коды.

Кроме того, используются арендованные на территории РФ серверы, сами же атаки проводятся в московском часовом диапазоне с учетом рабочего времени, выходных и праздничных дней.

Таким образом фабрикуются улики, включая IP-адреса и другие сведения технического характера. В дальнейшем выводы по работе следственных комиссий или

ангажированных компаний в сфере кибербезопасности без какой-либо объективной доказательной базы продвигаются через СМИ, в том числе в виде утечек и конфиденциальных бесед «с лицами, близкими к расследованию», а уже оттуда вирусно распространяются по социальным сетям.

В аналитическом отчете «Информационная война против России. Конструирование образа врага» компании АО «Крибрум», подготовленном по заказу Центра политической информации и выпущенном летом прошлого года, четко представлена технология, каким образом с применением последних достижений ИКТ и традиционной журналистики из России конструируется и экспортируется образ врага.

На первом этапе задействуется весь громадный потенциал западных корпоративных СМИ и подконтрольных социальных сетей для освещения и многократного тиражирования какого-либо события – в первую очередь киберинцидента, ответственность за который можно возложить на Россию. Так создается негативный образ России в восприятии жителей зарубежных стран.

После чего проводится экспорт сложившегося образа врага в российский сегмент информационного пространства. Далее через русскоязычные информационные ресурсы на Украине, в Грузии, Прибалтике, Израиле, а также «пятую колонну» внутри страны формируется негативное общественное мнение российских граждан по отношению к руководству РФ, госинститутам.

Против России ведется планомерная жестокая война, целью которой является уничтожение национальной идентичности, традиционных ценностей и государственности. Она идет с применением новейших достижений информационно-коммуникационных технологий и методов онлайн-журналистики, маскируясь под поток информационно-развлекательного контента. Такое коварство далеко не всегда удается своевременно распознать. В результате этот «троянский конь» спокойно въезжает в наши дома и сознание. Получается, что практически в прямом эфире происходит убийство нашего мировоззрения, памяти о прошлом. А значит, мы просто обязаны уметь распознавать врага в лицо, быть готовыми к идеологической схватке с ним.

Сергей Коротков, кандидат военных наук