И.Н. КОХТЮЛИНА

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ОСНОВНЫЕ УГРОЗЫ

Кохтюлина Ирина Николаевна, *к.полит.наук,*
Ответственный секретарь Научного совета
Национального института исследований глобальной безопасности
(НИИГлоБ), член-корреспондент РАЕН. E-mail: kin@niiglob.ru

Аннотация

Статья посвящена использованию социальных медиа в качестве «мягкой силы 2.0», понимаемой автором как эффективный инструмент для достижения политических целей государства, в частности, для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию.

Ключевые слова: *социальные сети, международная информационная безопасность, мягкая сила, информационная война, цифровой медиадепартамент.*

В течение последнего десятилетия Россия последовательно и прагматично выстраивает отношения с мировым сообществом в области международной информационной безопасности, направленные на консолидацию усилий в противодействии угрозам в информационной сфере.

24 июля 2013 г. Президентом Российской Федерации утверждены «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г.» [8].

В «Основах» под международной информационной безопасностью (МИБ) понимается «такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры» [8, Статья 6].

В документе к числу основных приоритетов отнесено участие России в формировании механизмов международного сотрудничества в области противодействия угрозам

использования информационно-коммуникативных технологий (ИКТ) в террористических и экстремистских целях, в том числе для вмешательства во внутренние дела суверенных государств.

В целом «Основы» закрепляют стремление Российской Федерации к масштабному сотрудничеству в деле укрепления мер доверия в сфере применения ИКТ и повышения эффективности переговорного процесса в области формирования системы международной информационной безопасности.

В отличие от старой триады составляющих МИБ (военно-политическая, криминальная и террористическая) в «Основах» изменена их структура и иерархия: в этом документе говорится об «использовании информационных и коммуникативных технологий

1) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;
2) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;
3) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;
4) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ».

В рамках настоящего доклада хотелось бы подробнее остановиться на третьей составляющей МИБ.

Ведущие страны мира разработали и реализуют стратагемы глобального информационного доминирования, в том числе через концепцию «мягкой силы»[1], то есть привлекательности и убеждения, а не принуждения.

Термин «soft power» – «мягкая сила» (имеются и иные варианты перевода) вот уже несколько лет пребывает в топ-листе тем, обсуждаемых научно-экспертными и политико-дипломатическими кругами. Помимо того, что у него имеется несколько вариантов перевода на русский язык, в литературе представлен ряд родственных терминологических инноваций, содержательные нюансы которых нуждаются в особом обсуждении, не входящем в задачи данной статьи.

Для небольших государств «мягкая сила» – это синоним эффективности соотношения ограниченных ресурсов влияния и дипломатического успеха, а также инновационности, экологичности и т.д.

В силу этого термин «soft power» оказывается потенциально совместимым с весьма разнообразными толкованиями, и это не в последнюю очередь обусловливает его популярность. Так, Дж. Най[2], введя его в предвыборные дискуссии в США, оказался убедительным и для республиканцев, и демократов.

Дж. Най понимал под властью способность добиваться желаемых результатов следующими тремя путями: принуждение, подкуп и привлекательность. Два первых подпадают под понятие жесткой власти, в то время как привлекательность – это признак мягкой

[1] «Мягкая сила» – форма политической власти, способность добиваться желаемых результатов на основе добровольного участия, симпатии и привлекательности, в отличие от «жёсткой силы», которая подразумевает принуждение.

[2] Джозеф С. Най-младший (Joseph S. Nye, Jr.; род. в 1937 г.) – американский ученый-международник, представитель неолиберализма, профессор Школы государственного управления им. Дж.Ф. Кеннеди в Гарвардском Университете. Впервые ввёл в оборот термин «мягкая сила» (англ. soft power) в своей книге «Bound to Lead: The Changing Nature of American Power» (1990 г.). Впоследствии развил данное понятие в книге «Soft Power: The Means to Success in World Politics» (2004 г.) и др. работах, некоторые из которых существуют в русских переводах.

власти. Следует особо подчеркнуть, что, вводя термин «мягкая сила», Най указывал на недостаточность использования одного из этих двух базовых ресурсов отдельно от другого.

С учетом современных реалий дефиниция «мягкой сила» неоднократно конкретизировалась и уточнялась, а стремительное развитие ИКТ способствовало подтверждению её эффективности как инструмента для достижения политических целей государства. Многие аналитики отмечают, что 2010 г. стал важной вехой для развития фактора «мягкой силы, так как именно этот период называют переходным от дебатов к количественному и качественному измерению данного фактора [15;16].

Изучением степени использования фактора «мягкой силы» различными государствами вот уже несколько лет занимаются английский независимый Институт управления и журнал «Монокль». В составленном рейтинге использования «мягкой силы» в 2014–2015 гг. 1-е место присуждено США, 2-е – Германии, 3-е – Великобритании. Китаю отведено 19-е место, России – 29 место [15].

Следует отметить, что одним из важных критериев, без которого было невозможно в полной мере определить влияние «мягкой силы» государства, стали различные количественные показатели: в частности, анализируются данные о количестве подписчиков на Twitter-аккаунты внешнеполитических ведомств и министров иностранных дел исследуемых стран.

В этом контексте, «мягкая сила 2.0.» сегодня (ср. [10]) может рассматриваться как метод переформатирования геополитического ландшафта планеты с помощью информационно-коммуникационных технологий (ИКТ): стратагемы непрямых действий и контролируемой нестабильности (управляемого хаоса) являются эффективными средствами ведения политической борьбы на международной арене, которые используются в целях ослабления реальных и потенциальных противников.

В новой редакции (от 12 февраля 2013 г.) Концепции внешней политики Российской Федерации [4, п. 20] впервые введено понятие «мягкой силы», понимаемой как комплексный инструментарий решения внешнеполитических задач с опорой на возможности гражданского общества, ИКТ, гуманитарные и другие альтернативные классической дипломатии методы и технологии. Обращено внимание на риски, связанные с деструктивным и противоправным использованием «мягкой силы» в целях оказания политического давления на государства, вмешательства в их внутренние дела, манипулирования общественным мнением и сознанием.

В Концепции рассмотрены меры, которые могут быть применены в интересах обеспечения национальной и международной информационной безопасности (пп. 32з–32и), предотвращения угроз политической, экономической и общественной безопасности РФ, возникающих в информационном пространстве, для борьбы с терроризмом и иными криминальными угрозами в сфере применения ИКТ, противодействия их использованию в военно-политических целях, противоречащих международному праву, включая действия, направленные на вмешательство во внутренние дела, а также представляющие угрозу международному миру, безопасности и стабильности. Учитывая особую важность этой проблемы, Россия будет добиваться выработки под эгидой ООН правил поведения по обеспечению МИБ.

В этом контексте, в выступлении Президента России В.В. Путина на заседании Коллегии ФСБ России 26 марта 2015 г. отмечено, что сегодня «для так называемого сдерживания России используется весь набор средств – от попыток политической изоляции и экономического давления до масштабной информационной войны и инструментов специальных служб» [1].

Им также было подчеркнуто, что «количество кибератак на официальные сайты и информационные системы органов власти России не уменьшается, только в прошлом году их пресечено около 74 млн. Кроме того, выявлено свыше 25 тыс. Интернет-ресурсов с публикациями, нарушающими закон. Прекращена работа более 1,5 тыс. экстремистских сайтов. Нужно продолжать очищать российское интернет-пространство от незаконных, преступных материалов, более активно использовать для этого современные технологии, участвовать в формировании системы международной информационной безопасности.

Речь идёт о том, чтобы обеспечивать безопасность и соблюдение законности, строго соблюдать российские и международные правовые нормы и стандарты в данной сфере. Не препятствовать общению людей в сети и размещению там законной, допустимой и корректной информации» [1].

Напомню, социальные сети стартовали в 1995 г., в них в настоящее время насчитывается уже более 2 млрд аккаунтов. Главное, что они позволяют, – это самовыражение и общение «многих со многими».

Повышение эффективности информационного управления в социальных сетях – одна из самых сложных задач в вопросе обеспечения национальной безопасности. Один из вариантов представлен на *Рисунок*.

Рисунок

Например, чтобы вывести какое-то событие в тренды в Twitter, нужно сделать, условно говоря, 4-5 тыс. перепостов с каким-то тегом. Этот тег попадет в тренд, где и продержится полдня. Про него напишут СМИ, в него поверят миллионы граждан, и новость станет общенациональной.

Принимая во внимание огромный интерес пользователей Интернет к соцсетям, становится очевидным, что они в настоящее время все активнее претендуют на роль «абсолютного оружия» в информационной войне, развязанной против России США и НАТО.

В соответствии с американской доктриной сетецентрических военных действий (Network Centric Warfare), в которой так называемая инфосфера рассматривается как полноценная арена боевых действий наряду с сушей, водой, воздухом и космосом, в структуре ряда американских правительственных и околоправительственных организаций формируются «центры цифрового противостояния России». Согласно планам, они будут действовать автономно, но в информационной координации друг с другом. А в случае получения соответствующей боевой задачи объединят усилия для массированной информационной атаки [3].

Следует отметить, что центральной задачей ведения всех сетецентрических войн является «совокупность действий, направленных на формирование модели поведения друзей, нейтральных сил и врагов в ситуации мира, кризиса и войны». Это предполагает заявку на установление контроля над всеми участниками актуальных или возможных боевых действий и манипулирование ими (в идеале тотальное) во всех ситуациях – и тогда, когда война ведется, и тогда, когда она назревает, и тогда, когда царит мир (см. [5]).

Концепция сетецентрической войны естественным образом включила в себя и достаточно давнюю уже стратегию непрямых действий, и трансформацию взглядов на ноополитику (первоначальная версия которой была теоретически обоснована в конце 1990-х гг., см. [12]), и сформулированную в 2002 г. Дж. Бушем-мл. доктрину упреждающих действий (Doctrine of Preemption, см. [14]). Она также отражает место и роль технологий информационного противоборства как инструмента, направленного на достижении глобальной гегемонии США во всех сферах мирового пространства, а также претензию на установление окончательного диктата по отношению ко всему мировому сообществу, включая и нынешних союзников по НАТО.

Основные задачи по ведению информационной войны с Россией в соцсетях возложены на американское разведсообщество и Пентагон. Так, директор ЦРУ Джон Бреннан недавно объявил о крупнейшей реорганизации ведомства со времен его создании в 1947 г., ключевым элементом которой станет создание Директората цифровых инноваций (Directorate of Digital Innovation) [13]. Он объединит такие прежде самостоятельные структуры, как Центр изучения открытых источников (Open Source Center), занимающийся мониторингом и анализом социальных сетей и блогосферы, и Центр информационных операций (Information Operations Center) – второе по величине подразделение ЦРУ, ответственное за кибершпионаж и информационные диверсии. Активными исследованиями по «прикладному использования соцсетей» занимается также Агентство перспективных исследовательских проектов разведсообщества США (Intelligence Advanced Research Projects Activity, см. [9]).

Задача – «повысить боевую активность в соцсетях», которые отныне рассматриваются в качестве «плановой рабочей зоны» с использованием специального программного обеспечения, позволяющего создавать фиктивных пользователей в Twitter, Facebook и др. сервисах в интересах «распространения свободы и продвижения демократических ценностей». Пункт управления спецоперациями в соцсетях располагается на базе ВВС США «Макдилл» (штат Флорида) и функционирует в режиме 24/7, личный состав – свыше 500 операторов, контролирующих около 100 фиктивных юзеров соцсетей, зарегистрированных в различных странах мира [3]. Безопасность их работы обеспечивает многоуровневая защита.

В 2015 г. на базе чешского офиса Radio Free Europe / Radio Liberty (Радио «Свобода», финансируется федеральным бюджетом США) запланировано создание цифрового медиадепартамента (DIGIM). В этом подразделении будут работать специалисты по соцсетям, основная задача которых – «противостоять дезинформации в российской медиасфере посредством различных соцмедиаплатформ (в частности, Facebook, Twitter, «ВКонтакте» и «Одноклассники»)». О создании киберштаба в Праге говорится в подробной заявке американской правительственной организации Совета управляющих по вопросам вещания (Broadcasting Board of Governors; BBG) на следующий финансовый год, начинающийся с 1 октября 2015 г. Заявка подана от лица президента США в конгресс в марте 2015 г. [7].

Примечательно, что Совет управляющих по вопросам вещания (BBG) объединяет Радио «Свободная Европа»/Радио «Свобода» (RFE/RL), «Голос Америки» (VoA) и другие государственные медиаканалы США; уставная цель данной организации – распространение информации «в странах, где есть недостаток независимых СМИ».

России в 160-страничной заявке BBG посвящен раздел «Противодействие реваншистской России», где изложены планы на 2015–2016 гг. и названы причины, по которым необходимо вести информационную борьбу с Россией.

В заявке, в частности, отмечено, что Россия «запустила всемирный механизм дезинформации», его «цель – не убедить (как в классической общественной дипломатии) и заслужить доверие, а посеять смуту теориями заговора и распространить ложь» и что «Кремль использует свободу информации для внедрения дезинформации», применяет информацию, чтобы «запутать, деморализовать, извратить, парализовать и создать альтернативную реальность», а также что «демократия в России в опасности и ей грозит нестабильность» [12, p. 16].

BBG указывает на расширение своей активности в Интернете, в частности в социальных сетях. В списке соцсетей, где будет вестись работа, – «Одноклассники», пользователи которой наиболее активно отстаивают официальную позицию России по многим вопросам. Кроме борьбы в классических социальных сетях, новая команда будет использовать мессенджер WhatsApp «в качестве мобильной платформы с push-сообщениями для привлечения новой аудитории».

Основным оружием в информационной борьбе с Россией, по мнению разработчиков проекта создания киберштаба в Праге, должны стать оригинальные программы и политическая сатира. В рамках нового представительства США в российских соцсетях запланирован видеопроект Footage vs. Footage («Съемка против съемки») – ежедневный продукт, изобличающий «российскую телевизионную пропаганду», а также канал на YouTube и сайт Rus2Web – площадка для российских журналистов и кинематографистов, чья работа сейчас «блокируется Кремлем».

Рекламировать Радио «Свобода» и «Голоса Америки» в русскоязычном сегменте интернета будет Интернет-портал Google.

В качестве главных достижений за 2014 и 2015 гг. в информационной борьбе с Россией BBG указывает предоставление объективных новостей об Украине, освещение присоединения Крыма к России в таких программах, как «Донбасская реальность» – еженедельная 30-минутная программа о событиях в Донбассе, транслируемая на украинском «Донбасс-ТВ», и «Крымская реальность» – еженедельная 20-минутная программа о развитии «аннексированного Россией полуострова», программу показывает украинский канал «24».

В запросе BBG на текущий финансовый год было указано, что медиаканалы CCTV (Китай), Russia Today и Al Jazeera вторгаются в западное новостное пространство и «умело формируют лояльную аудиторию», отбирая зрителей и слушателей у американских медиа. В силу этого на следующий финансовый год (с 1 октября 2015 г.) на проект по борьбе с «реваншистской Россией» в BBG собираются затратить 15,6 млн долларов США. Данный проект определен BBG как приоритетный наравне с противостоянием идеологии фундаменталистов из запрещенного в Российской Федерации «Исламского государства» (ИГИЛ) (на него запрошено 6,1 млн долл.). Всего на 2016 финансовый год BBG запросила у конгресса США бюджет в 751 млн долл. (+1 % к предыдущему году). В целом на русскоязычное вещание RFE/RL будет выделено на 250 тыс. больше – 7,4 млн долл. [7].

Следует отметить, что ни «Голос Америки», ни Радио «Свобода» сейчас не осуществляют радиовещания в России. «Голос Америки» лишился частоты 810 кГц в начале 2014 г., что касается Радио «Свобода», то оно прекратило вещать в 2012 г. Радиостанции полностью ушли в Интернет.

Присутствие в российском телеэфире запланировано увеличить путем сотрудничества «Голоса Америки» с российским холдингом РБК. Таким образом, BBG упорно старается продвинуть американскую позицию на российские телеканалы, выбирая для партнерства, как правило, оппозиционные телеканалы и новостные ресурсы. К примеру, в заявке на 2014 финансовый год также упоминалось, что «Голос Америки» запустил видеопрограмму «Поделись», которая нацелена на «молодежную аудиторию будущих лидеров» и предлагает «современную дискуссию об Америке и ее ценностях, политике США и постсоветскую эру для современного зрителя». В числе партнеров «Голоса Америки» в материалах BBG указывался ресурс «Грани.ру» и телеканал «Дождь».

В этой связи в российском Национальном центре управления обороной государства (НЦУОГ), ведущем мониторинг соцсетей, уже зафиксирована активизация информационной работы из-за рубежа против России и ее военно-политического руководства [6]. Установлено, что большинство участников информационных атак – русскоязычные украинские блогеры. В НЦУОГ также обращают внимание на низкопробность многих подобных материалов, при этом отмечая их массовость и быстроту распространения в блогосфере.

В то же время весной 2015 г. Европарламент предложил Еврокомиссии и странам ЕС заняться поиском СМИ и организаций-российских агентов, готовить планы противодействия российской информационно-пропагандистской активности в СМИ и усилить помощь российским НПО [2].

Такая инициатива содержится в принятом докладе комитета Европарламента по иностранным делам, на основании которого должна быть разработана резолюция по пересмотру отношений с Россией, включающем:

- разработку механизма для сбора, мониторинга и выявления финансовой, политической и технической помощи, предоставленной Россией политическим партиям и другим организациям в составе ЕС, с целью оценки ее влияния на политическую жизнь и дебаты в ЕС;

- политическую и финансовую поддержку независимых (по мнению Европарламента) организаций активистов гражданского общества, СМИ и НПО в России и установку контактов с организациями и лицами, которые склонны развивать альтернативное видение политических и дипломатических отношений с ЕС.

Таким образом, становится очевидным единый замысел и целенаправленная системная деятельность в ведении гибридной войны, где основная составляющая – информационная. В этой связи представляется оправданным дополнить основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации (утверждены Совбезом России 07.03.2008) проблематикой исследований вопросов информационного влияния, информационного управления и информационного противоборства (в том числе, с использованием социальных сетей) на межгосударственном, национальном, региональном, территориальном, отраслевом и корпоративном уровнях.

INTERNATIONAL INFORMATION SECURITY: THE MAIN THREATS

***Irina N. Kokhtyulina**, PhD, Executive Secretary of Scientific Council*
National Institute of Global Security Research
Corresponding Member of Russian Academy of Natural Science
E-mail: kin@niiglob.ru

Summary

The article describes principles and methods of using social media as a «soft power 2.0» which is considered as an effective tool to achieve political goals of the state.

Particularly increasing today is the risk of destructive informational influence threatening the sovereignty and territorial integrity of any state. As a consequence, individuals and society as a whole are also exposed to negative information impact.

Key words: *social networks, the international information security, soft power, information warfare, digital media department.*

ЛИТЕРАТУРА/REFERENCES

1. Выступление В.В. Путина на заседании Коллегии ФСБ России 26.03.2015. [Электронный ресурс]. URL: http://kremlin.ru/events/president/transcripts/49006
2. Европарламент предложил странам ЕС заняться поиском СМИ и организаций-российских агентов. [Электронный ресурс]. URL: http://tass.ru/mezhdunarodnaya-panorama/1961600
3. Злобнецкий Н. Поле битвы – соцсеть. [Электронный ресурс]. URL: http://stringer-news.com/publication. mhtml?Part=48&PubID=34840)
4. Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В.В. Путиным 12 февраля 2013 г.). ([Электронный ресурс]. URL: http://www.mid.ru/ foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/122186).
5. *Коровин В.* Главная военная тайна США. Сетевые войны. – М.: Яуза: Эксмо, 2009. 288 с. (Войны XXI века).
6. *Мухин В.* Пентагон набирает кибербойцов по всему миру. [Электронный ресурс]. URL: http://www.ng.ru/world/ 2015-04-03/2_ pentagon.html
7. *Нечаев В., Амирджанян М., Подрез Т.* США вводят информационные войска в российские социальные сети. [Электронный ресурс]. URL: http://izvestia.ru/news/585366
8. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утверждены Президентом Российской Федерации В.В. Путиным 24 июля 2013 г., № Пр-1753). [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/6/114.html
9. *Платов В.* Изучение социальных сетей в интересах спецслужб США. [Электронный

ресурс].URL: http://ru.journal-neo.org/2015/01/03/izuchenie-sotsial-ny-h-setej-v-interesah-spetssluzhb-ssha.
10. *Смирнов А.И., Кохтюлина И.Н.* Глобальная безопасность и «мягкая сила 2.0»: вызовы и возможности для России – М.: ВНИИгеосистем, 2012.
11. *Arquilla J., Ronfeldt D.* The Emergence of Noopolitik. Toward An American Information Strategy. RAND Report, 199. URL: http://www.rand.org/pubs/monograph_reports/ MR1033.html
12. Fiscal Year 2016 Congressional Budget Request. Broadcasting Board of Governments. URL: http://www.bbg.gov/wp-content/media/2015/03/FY2016Budget_CBJ_Final_Web Version.pdf
13. *Miller G.* CIA plans major reorganization and a focus on digital espionage // The Washington Post, URL: https://www.washingtonpost.com/world/national-security/cia-plans-major-reorganization-and-a-focus-on-digital-espionage/2015/03/06/87e94a1e-c2aa-11e4-9ec2-b418f57a4a99_story.html.
14. The National Security Strategy of the United States of America. September 2002. URL: http://www.state.gov/documents/organization/63562.pdf
15. The New Persuaders III. A 2012 Global Ranking of Soft Power / By J. McClaury. URL: http://www.instituteforgovernment.org.uk/sites/default/files/publications/The%20new%20persuaders%20III_0.pdf
16. Soft Power Survey 2014/15. URL: http://monocle.com/film/Affairs/soft-power-survey-2014-15/