ДУКИН РУСЛАН АЛЬБЕРТОВИЧ

СОЦИАЛЬНЫЕ МЕДИА КАК ИНСТРУМЕНТ СОВРЕМЕННЫХ ВОЙН И УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ

АННОТАЦИЯ

Дана характеристика современных гибридных войн. Определена и рассмотрена роль социальных медиа в качестве инструмента информационных войн. Представлены примеры угроз информационной безопасности России, которые возникают посредством социальных медиа.

Ключевые слова: социальные медиа; информационная безопасность; гибридная война.

DUKIN R. A.

SOCIAL MEDIA AS A TOOL OF MODERN WARS AND INFORMATION SECURITY THREAT OF RUSSIA

ABSTRACT

The characteristic of modern hybrid wars is given. The role of social media as a tool of information wars is defined and considered. Examples of information security threats of Russia, which arise through social media, are submitted.

Keywords: social media; information security; hybrid war.

Современные войны в корне отличаются от войн XX столетия или начала XXI века. Существенно изменились стандарты и методы ведения войны: глобально акцент сместился от летальных средств *истребления* к нелетальным способам *подавления*. Современные войны принято называть гибридными или неконвенциональными. Их характерной особенностью является одновременное применение самых разных технологий, а также сочетание «мягкой» и «жесткой» силы.

«Гибридная война» – не новый, но актуальный способ подавления соперника. В редакторском предисловии справочника Military Balance термин «гибридная война» трактуется как «использование военных и невоенных инструментов в интегрированной кампании, направленной на достижение внезапности, захват инициативы и получение психологических преимуществ, использующих дипломатические возможности; масштабные и стремительные информационные, электронные и кибероперации; прикрытие и сокрытие военных и разведывательных действий; в сочетании с экономическим давлением» [1].

Ключевой момент в этом определении – «использование военных и невоенных инструментов в интегрированной кампании». Суть современных войн заключается не столько в физическом истреблении армии противника или разрушении его инфраструктуры, сколько в создании условий, при которых соперник окажется проигравшим, даже не вступив в «открытый бой». Развитие военных технологий привело к ситуации, когда прямое столкновение двух развитых в военном плане сторон может привести к катастрофическим последствиям для всей планеты. Поэтому летальное вооружение применяется точечно,

а «реальные» бои сошли с глобального уровня на локальный. Вместе с тем, война по-прежнему оказывает огромное влияние на массы людей – в условиях современной войны «происходит милитаризация общественного сознания и сжатие демократических институтов» [2, с. 108].

Любую современную (гибридную) войну можно рассматривать в контексте ее составных частей, к которым можно отнести:

- информационные войны (посредством СМИ и социальных медиа);
- кибернетические войны (хакерские атаки, взлом электронных систем, кража данных);
- экономические войны (экономические санкции, искусственные торговые ограничения, моратории на инвестиционную активность, «перекачивание» научного потенциала);
- политические войны (политические санкции, создание условий для политической изоляции).

В цифровую эпоху особую опасность представляют информационные и кибернетические войны. Понятие «информационная безопасность» заметно расширилось в третьем тысячелетии и в современном социуме имеет две составляющие: информационно-техническую безопасность и информационно-психологическую. Первая составляющая подразумевает под собой искусственно созданный человеком мир технологий, вторая составляющая – естественный мир живой природы, куда входит и сам человек.

Важность обеих составляющих информационной безопасности в современной России чрезвычайно высока. Информационные угрозы представляют серьезную опасность для Российской Федерации – молодого государства, которое не до конца институционализировало собственные национальные интересы и находится в стадии трансформации. Именно по этим причинам в 2014 году на военно-научной конференции Академии военных наук Начальник Генерального штаба Вооруженных Сил Российской Федерации Валерий Васильевич Герасимов особо отметил опасность информационных угроз, заявив, что «военные действия смещаются в информационное и космическое пространство» [3].

После утверждения Президентом РФ нового Положения о генеральном штабе было сообщено о создании в Вооруженных силах Российской Федерации войск информационных операций, в состав которых вошли подразделения, укомплектованные математиками, программистами, инженерами, криптографами, связистами и другими специалистами. Главные задачи этой воинской структуры – обеспечение кибербезопасности информационных сетей России и нарушение работоспособности информационных сетей вероятного противника. К примеру, в США подобное подразделение было создано еще в 2009 году и называется «Кибернетическое командование» (USCYBERCOM). «Кибернетическое командование» отвечает за все операции США в области кибербезопасности и возглавляется непосредственно директором Агентства национальной безопасности США.

Очевидно, что и «Кибернетическое командование» США, и войска информационных операций РФ, обеспечивают, прежде всего, информационно-техническую безопасность своих государств. Однако вторая составляющая общей информационной безопасности – информационно-психологическая – также требует пристального внимания со стороны государственных структур. Развитие медиа и интернет-технологий привело к созданию мощнейшего инструментария, способного воздействовать на массовое сознание в глобальных масштабах. Основным информационным «оружием» в наше время стали социальные медиа.

Социальные медиа – это «группы интернет-приложений на той или иной идеологической и технологической базе Web 2.0, позволяющих участникам общения в социальных сетях создавать содержание в процессе обмена им» [4, p. 60]. Социальные медиа имеют ряд радикальных отличий от традиционных видов медиа, обладая, в частности, гораздо большим управленческим потенциалом. Поскольку социальные медиа апеллируют к чувству принадлежности человека к тому или иному сообществу, они имеют огромное влияние на его социализацию и мировоззрение.

Социальные медиа в современном понимании – феномен молодой и многими специалистами в области безопасности недооцененный. Между тем, социальные медиа проникли абсолютно во все сферы общественной жизни – фактически можно констатировать их институционализацию в российском социуме. Пользование социальными медиа стало повседневной практикой, что привело к стиранию границы между реальностью и виртуальностью.

Контаминация реального и виртуального характерна и для военного дискурса. Одной из существенных особенностей современной информационной

войны является «отсутствие четких пространственно-временных границ» [5]. Например, если в XX веке понятия «фронт» и «тыл» имели географические маркировки, то в современности эти понятия практически утратили какую-либо физическую привязку. Интерпретация «фронта» зависит от уровня абстрагирования: в информационном пространстве проводятся информационные «атаки» и взрываются информационные «бомбы». Если противника не победить блицкригом, ему организуют информационную «блокаду».

В основе информационных войн лежат опробованные десятилетиями методы пропаганды и «промывки мозгов». В условиях глобализации и развития социальных медиа они приняли форму оружия массового поражения. Медиа в информационных войнах используются как эффективные каналы передачи нужных образов и смыслов, поэтому такие войны часто называют *смысловыми*.

Главная цель смысловой войны – разрушить прежнюю картину мира потенциального противника и сподвигнуть его на решения, которые он не принял бы при прежней картине мира. Атакам подвергается конкретный человек – актор и потребитель информации. Социальные медиа как самый массовый вид коммуникации позволяет организовать специфический виртуальный менеджмент, с помощью которого можно контролировать поведение не только конкретного человека, но и целых социальных групп, поскольку главный принцип социально-медийных платформ основан на добровольном создании сообществ по интересам.

Социальные медиа в таком контексте являются невоенным инструментарием войны, а также институциональным полем, содержащим огромное количество реальных угроз для информационной безопасности Российской Федерации. Борьба с этими угрозами осложнена многими факторами, в том числе и особенностями структуры социальных медиа – отследить появление и распространение разрушительной информации физически не всегда возможно. А полный запрет использования социальных медиа внутри страны исключен по понятным причинам. Кроме того, зачастую информационные «бомбы» имеют долгосрочный характер действия, и, мимикрируя под социально одобряемые формы, проходят мимо внимания объекта атаки. Таким образом, главная проблема для информационной безопасности государства в такой ситуации является отсутствие по-настоящему действенных механизмов контроля над информацией, которая распространяется в социальных медиа.

Типологию информационных угроз России в социальных медиа можно проиллюстрировать конкретными примерами:

– *Террористические угрозы*. Например, террористическая группировка ДАИШ, также известная как ИГИЛ (*организация запрещена в России*), занимается вербовкой новых бойцов через социальные медиа. В российском интернет-сегменте активность ДАИШ очень велика: в одной только социальной сети ВКонтакте существуют десятки сообществ и сотни персональных страниц, где можно зафиксировать пропагандистскую деятельность террористов. Для русскоязычной аудитории также активно используются социальные платформы Facebook и Twitter, на которых боевики разворачивают агрессивную информационную кампанию в духе поп-культуры, с использованием сюжетов из видеоигр и кинофильмов. Очевидно, что целью террористов являются молодые девушки и юноши. Конечно, страницы и аккаунты с запрещенной информацией блокируются по требованию Генпрокуратуры, однако вместо них тут же появляются новые.

– *Угрозы информационному суверенитету*. В данном случае имеется в виду внедрение иностранных агентов в информационное пространство государства. В частности, по сообщению газеты «Известия» [6], в 2015 году США ввели «информационные войска» в российский сегмент социальных медиа. На базе чешского офиса Radio Free Europe создан цифровой медиадепартамент DIGIM, в котором работают специалисты по социальным сетям. Их задачей является противодействие дезинформации в российской медиасфере посредством различных соцмедиаплатформ (Facebook, Twitter, ВКонтакте и Одноклассники). Создание кибершатаба в столице Чехии подтверждается заявкой американской правительственной организации Совет управляющих по вопросам вещания (Broadcasting Board of Governors; BBG) на финансовый год с 1 октября 2015 года [7]. Уставная цель BBG – распространение информации в странах с недостатком независимых СМИ. В заявке BBG Российской Федерации отводится целый раздел под названием «Противодействие реваншистской России».

– *Угрозы конституционному строю России*. Социальные медиа предоставляют площадку для объединения различных экстремистских и ультрарадикальных сил, целью которых является свержение действующей политической власти либо

акты сепаратизма. В подобном ключе действуют не только маргинальные (в социологическом смысле) элементы, но и некоторые фонды и организации, признаваемые впоследствии иностранными агентами. Часто используются информационные «вбросы», дезинформация, диффузия смыслов, смещение информационных акцентов, передергивание фактов и другие пропагандистские приемы. Подобную тактику можно проследить на примере интернет-пользователей из Украины. Вследствие ухудшения российско-украинских отношений некоторые из них проводят информационные атаки в русскоязычном сегменте социальных медиа. Это зачастую сопровождается визуальными материалами, которые провоцируют сепаратистские настроения среди различных национальных групп, проживающих на территории Российской Федерации. Стоит отметить, что часть российских интернет-пользователей отвечают аналогичным образом, что подтверждает тезис о том, что социальные медиа – это «поле боя» современных информационных войн.

Конечно, помимо вышеперечисленных угроз существуют и другие. В частности, угрозы личной безопасности человека или угрозы разжигания различных видов розни. Социальные медиа репрезентируют современное общество риска – социум, в котором человек постоянно находится в состоянии каких-либо угроз. Стратегическая задача государства – свести эти угрозы к минимуму. Выполнение этой задачи осложнено по объективным причинам, но очевидно, что необходима единая концепция информационной безопасности в части социальных медиа.

Во-первых, необходимо разработать механизм, который позволил бы быстрее реагировать на появление и распространение противозаконной информации в социальных медиа. Существующий механизм слишком неповоротлив и бюрократичен – зачастую удаление экстремистских материалов происходит спустя значительное количество времени, когда «целевая аудитория» уже получила месседж. Во-вторых, необходима структура, которая занималась бы охраной информационного пространства в русскоязычном сегменте социальных медиа, что подразумевает не цензуру, но противостояние информационным атакам «извне». В-третьих, очень мало созидательной работы со стороны государства в социальных медиа. Информационное пространство можно и нужно заполнять качественными медийными проектами, что является не только хорошей профилактикой среди интернет-пользователей, но и важным стратегическим ресурсом для страны.

Список литературы

1. Military Balance 2015 Press Statement [Электронный ресурс]. – Режим доступа: https://www.iiss.org/en/about%20us/press%20room/press%20releases/press%20releases/archive/2015-4fe9/february-0592/military-balance-2015-press-statement-40a1 (дата обращения 20.12.2015).
2. *Яницкий О. Н.* Современные войны: социально-экологическое измерение // Вестник Института социологии. – 2014. – №11. – С. 106–126.
3. *Герасимов В. В.* Генеральный штаб и оборона страны [Электронный ресурс] // Военно-промышленный курьер. – 2014. – Режим доступа: http://vpk-news.ru/articles/18998 (дата обращения 20.12.2015).
4. *Kaplan A. M., Haenlein M.* Users of the world, unite! The challenges and opportunities of Social Media // Business Horizons. – 53 (1) – P. 59-68.
5. *Лабуш Н. С.* Информационная война как порождение нового времени и современных массмедиа технологий. Часть II. Контуры информационной войны современности [Электронный ресурс] // Медиаскоп. – 2015. – Вып. 2. – Режим доступа. – http://www.mediascope.ru/node/1739 (дата обращения 20.12.2015).
6. США вводят информационные войска в российские социальные сети [Электронный ресурс] // «Известия». – 14.04.2015. – Режим доступа: http://izvestia.ru/news/585366 (дата обращения 20.12.2015).
7. Budget Submissions: Broadcasting Board of Governors [Электронный ресурс]. – Режим доступа: http://www.bbg.gov/about-the-agency/research-reports/budget-submissions (дата обращения 20.12.2015).