ИНФОРМАЦИОННАЯ ВОЙНА, И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

Д.Н. Беспалов, М.А. Казаков

НИУ ВШЭ, 101000, Москва, ул. Мясницкая, д.20
ННГУ, 603950, Нижний Новгород, пр. Гагарина, д.23

В статье представлены противоположные, но взаимосвязанные реальности – информационная война и информационная безопасность, цели и задачи их изучения в рамках схемы «вызов-ответ», методологическое и аналитическое обеспечение, роль элит и информационного общества в продвижении информационной безопасности.

Одной из черт современности является глобальное распространение информационно-коммуникационных технологий (ИКТ), сочетающееся в ряде стран с неэффективным управлением и иными трудностями в строительстве базирующихся на них инновационных инфраструктур. Это приводит к воспроизводству угроз, прежде всего связанных с возможностью использования ИКТ в целях, несовместимых с задачами: поддержания международного мира и безопасности; соблюдения принципов отказа от применения силы; невмешательства во внутренние дела государств и т.п. В связи с этим фигурируют такие термины, как «угроза информационных войн», «информационный терроризм» и пр.

Информационные войны, где пребывание в политике объявляется борьбой за существование, а отношения определяются в терминах «друг–враг», «свой–чужой», превосходство над оппонентом или «захват его территории» является целью политической деятельности. Информационная безопасность в таком случае выступает как деятельность, аналогичная процессу политического управления, который включает совокупность компонентов гуманитарного характера. В этом контексте и само решение представляет собой отношение достигнутого результата информационно-политического воздействия к намеченной цели – формированию позитивного образа России. Приведение её политики в соответствие с запросами здорового общественного мнения способно обеспечивать проводимость инициатив власти внутри страны и повышать легитимность действий РФ в мире.

Ключевые слова: информационная война, коммуникация, манипуляция, пропаганда, информационная безопасность, информационное общество, общественное мнение, элита.

Одной из черт современности является глобальное распространение ИКТ, сочетающееся в ряде стран с неэффективным управлением и иными трудностями в строительстве инновационных инфраструктур, базирующихся на них. Это приводит к воспроизводству угроз, прежде всего связанных с возможностью использования ИКТ в целях, несовместимых с задачами поддержания международного мира и безопасности, соблюдением принципов отказа от применения силы, невмешательства во внутренние дела государств и т.п. В связи с этим фигурируют такие термины, как «угроза информационных войн», «информационный терроризм» и пр. Их суть заключается в том, что указанные явления способны вызвать информационные конфликты, чьи последствия могут быть сопоставимы с последствиями преступлений, угрожающих международному миру и безопасности [1, с. 792].

Анализ этих явлений делает настоятельным постоянное уточнение современных взглядов на структуру информации, взаимосвязь между нею и политикой, на природу явлений, известных под названием «информационная война» и «информационная безопасность», различающихся подходами к политике как таковой, стратегиями, вариантами воздействия и поведения. Для любого объекта, понятия главным является содержание, поэтому и для информации, и для её производных сущностью остаётся субъект, его восприятие объективной реальности, основанное на определённых целях, потребностях, интересах, что и подчёркивает социально-политический и гуманитарный характер информации.

Хотя угроза, которую информационная война представляет для безопасности стран, пока проигрывающих во включённости в глобализацию, нередко преувеличивается, её влияние на национальную политику, учитывая целый комплекс этнокультурных, религиозных и других цивилизационных конфликтов, будет лишь возрастать, что требует модификации существующих систем обеспечения безопасности. Ныне уже не только постмодернисты выражают мнение, что традиционные способы обеспечения национальной и международной безопасности не способны справиться с новыми угрозами. В их меняющейся иерархии угроза информационной войны, по аналогии с тем, как В.В. Путин охарактеризовал феномен «мягкой силы», это «…комплекс инструментов и методов достижения внешнеполитических целей без применения оружия, а за счёт информационных и других рычагов воздействия. ...Нередко эти методы используются для взращивания и провоцирования экстремизма, сепаратизма, национализма, манипулирования общественным сознанием, прямого вмешательства во внутреннюю политику суверенных государств» [3].

В рамках научной терминологии следует признать, что число «работающих» дефиниций собственно информационной войны в таком ключе не велико и опираются они на два основных методологических подхода к изучению современных конфликтов и войн [1, с. 92, 103–104, 126–127]. Первый базируется на сборе и анализе информации о параметрах конфликтов с упором на количественные, исчисляемые показатели. Второй – изначально нацелен на качественный анализ форм насилия и изменений в их характере.

Именно второй подход, учитывающий количественные показатели, но не абсолютизирующий их значения, дал науке и практике большее число знаковых теоретико-аналитических разработок. Он, в частности, своевременно отреагировал на то, что характер современных конфликтов меняется гораздо быстрее, чем системы их категоризации и учёта в базах данных, введя установки на развитие профессионального конструирования реальности [4]. В нашем случае субъекты, конструирующие угрозы в контексте актуальной для них системы значений, участвуют в борьбе за власть, конкурируя друг с другом за производство смыслов, как в сфере войны, так и безопасности.

Определение информационной войны (ИВ) как «коммуникативной технологии по воздействию на массовое сознание с кратковременными и долговременными целями» [5, с. 20–23] в очередной раз возводит элитарное сознание и его носителей в ранг творцов истории, ставших идоминирующих ныне за счёт далеко не открытой борьбы и политики. Для этих субъектов были b остаются актуальными вопросы, как эффективно воздействовать на аудиторию, как сохранить контроль над коммуникацией, как правильно манипулировать массами, чтобы удержать перевес своих сторонников.

Объективно такая ситуация связана с разной степенью развитости демократических институтов и гражданского (информационного) общества в странах мира. Кроме того, в каждой из них различаютсравнительно большие социальные слои, не имеющие по разным причинам возможности стать «современными людьми» (А. Инкельс). Поэтому у социума была и остаётся как бы ответная потребность: как удержать под контролем ускользающие информационно-политические коммуникации, не «попасть» под нарастающее манипулятивное воздействие власти, каким образом сохранять свою субъектность, получать адекватное представление о текущих процессах, месте и роли в них себя и других.

Такое состояние общества в целом даёт основание выделять и подчёркивать его особый статус как объекта воздействия, целью которого является внесение изменений в «когнитивную карту» управляемых, с тем чтобы получить соответствующие изменения в её механизмах, главное – в характере участия и структуре их поведения. На то же практически нацелено и политическое манипулирование. Поэтому другая часть определений ИВ связана со специфической формой массированного использования мани-

пулятивных технологий – особым способом перепрограммирования массового и индивидуального сознания в интересах гегемонии тех или иных политических акторов путём изменения сложившейся в сознании групп и индивида картины мира (А. Грамши и его последователи). Параллельно следует выгодное манипулятору структурирование реальности, задающее большинству не только алгоритм поведения, но и образ жизни.

Взаимосвязь этих подходов очевидна и наглядно представлена А.И. Соловьёвым: «Показателем безусловной крепости положения политической элиты служит и её способность к манипулированию общественным мнением, такому использованию идеологических и иных духовных инструментов, которые могут обеспечить требуемый уровень легитимности власти, вызвать расположение и поддержку со стороны общественного мнения» [6, с. 134].

В логике власти, то есть в обладании элитой всеми возможными в современном обществе способами управления, продолжается освоение ею возможностей Интернета. О чём свидетельствует и сетецентрический подход, который с конца 1990-х гг. будоражит умы не только военных, но и политиков. Тогда же на Западе и в России существовали немалые надежды на то, что массовое распространение Интернета позволит избежать манипулятивного воздействия СМИ, создать определённый противовес доминированию конгломератов технократии.

Этого не произошло. Более того, возможность создания сетевых организаций и появление информационных сетей породили новый тип войны – сетевой. Её цель – установление и поддержание со стороны соответствующего субъекта информационного превосходства над теми или иными (экономическими, политическими, культурными) процессами. Властная иерархия данный момент пропустила, в силу чего умелая координационная и пропагандистская работа, особенно в социальных сетях, создаёт ныне больше условий для быстрой мобилизации масс с целью начала революции, чем продвижения вглубь модернизации.

Интернет как информационная среда всё больше теряет демократичность и всё чаще выступает в виде инструмента односторонней самоорганизации, ложной героизации и манипуляции,причём конфликтов и войн, ведущихся не столько вовне и против кого/чего-либо, а, скорее, внутри и за.Последнее столь ёмкое, что в нём хватает места и смене элит(событиям, получившим название «цветных революций»), и операциям по спасению и развитию народов, которые могут быть, оказывается, «без стрельбы и крови».

Другими словами, формы, которые приобретает текущий процесс «войны и мира» с возрастающейм в нём информационной составляющей, требуют глубокой научной рефлексии. А проблема политических коммуникаций в их контексте, где манипулирование является общим механизмом, взывает к новым решениям, в связи с чем крайне остра необходимость создания интегративной модели для установления взаимосвязи когнитивных, социальных и политических процессов конструирования угроз, обусловленных новыми формами конфликтов.

С научной точки зрения, в изучении информационной войны актуальна сама верификация её концепции с целью достижения большей результативности политологических выводов, содействующих приращению знаний по её нейтрализации и повышению уровня полезности соответствующих исследований в познании существующих и потенциальных угроз. В частности, именно эти знания (образы, представления) выступают фундаментом системы информационной безопасности, объектом которой является информация, информационные технологии и методы их использования. Новые взгляды и понимания с опорой на принципы безопасности вкупе с изменениями в соотношении сил применяются для определения характера приоритетных угроз, закрепляются в правилах и нормах, практиках внешнеполитического и внутриполитического сотрудничества по управлению конфликтами.

Прошлое сделало понятие «информационная война» в отечественной науке мистифицированным и одновременно недостаточно систематизированным. Эта неопределённость его качественного составаискажает понимание такого явления, как феномен кризисной политики, его реальных параметров и системных связей. Сегодня он рассматривается в качестве одного из базовых по методологии воздействия в арсенале военно-политических и социально-коммуникативных исследований. Это делает переход от прежней мировоззренческой установки, согласно которой тотальность и изощрённость ИВ практически не оставляет объекту воздействия надежды на возможность реализации своих интересов, к иной, понимающей в соотнесении форм войны и мира ценности безопасности. Фактически кумулятивное влияние целого спектра изменений приводит к формированию новой культуры безопасности, носителями (производителями) которой выступают и политические элиты, и народы.

Она служит основой для осмысления значения традиционных и новых источников опасности, продуцируемых агентами войны, и организации инфраструктурных практик. Организационная их составляющая включает в себя производство средств информации и информационных услуг, информационный рынок, подготовку и переподготовку кадров, проведение научных исследований. Последние несут ответы не только академического, научно-технического, но и содержательно-технологического характера, национально и практически ориентированы.

Никогда не следует забывать, что идеи и технологии только тогда «дойдут» до адресата, когда

технико-технологическая составляющая, представленная информационно-телекоммуникационными системами и сетями связи, способна на производство эксклюзивного программного продукта. Наличие национальной операционной системы ––не только конкурентное преимущество, но и фактически решение проблем обеспечения информационной безопасности, где дифференцированные ответные меры есть и мощное средство воздействия на источники, передатчики, и способ объяснения обществу тех представлений, что поддерживают устойчивость политической системы.

Информационная война как реальность в рамках схемы «вызов-ответ», занимает то место в комплексе информационно-коммуникационных ресурсов, при помощи которых государство (или их коалиция) решается на проведение своей политики средствами информационного насилия. Специалисты выделяют 11 факторов, создающих опасность для основных интересов личности, общества и государства в информационном пространстве и представляющих, таким образом, непосредственные угрозы международной и национальной безопасности. Это, прежде всего:

– разработка и использование средств несанкционированного вмешательства в работу и неправомерного использования информационных ресурсов другого государства, а также нанесения ущерба им;

– целенаправленное информационное воздействие на критические инфраструктуры и население другого государства;

– действия, направленные на доминирование в информационном пространстве, поощрение терроризма и собственно ведение информационных войн.

Соответственно, используя совокупность международных и региональных организаций, приёмов и способов их действий, а также правовых, дипломатических, религиозных и этических норм, государство организует для упреждения, минимизации и ликвидации возможностей нанесения ущерба противостоящую им систему информационно-политических мер и мероприятий. Оно, использует для этого уместные каналы, структуры и инструменты и создаёт, в том числе и для себя, нужный масштаб коммуникации со всеми социальными слоями.

Уже классик теории политических коммуникаций Э. Бернейс использовал в качестве аргумента в защиту пропаганды (разграничения Г. Джоветта и В. О'Доннела) борьбу с инерцией обществ и в этой связи разработал концепцию общественного мнения как механизма изменения социума. Значение последнего определяется для него тем, что«авторитетные и влиятельные группы могут стать важными каналами для влияния на аудитории, превосходящие их по размерам. Чтобы преодолеть инерцию существующих традиций и установок, идеи необходимо подавать эффектно, а сценарии реализовывать с драматизмом»[7, с. 149].

В этом коммуникация противостоит традиции как институциональному механизму формирования общественного мнения, а также соответствующему представлению о нём как отношении к тем или иным текущим темам. Без манипуляции как его движущей силы общественное мнение, с точки зрения Бернейса, функционировать не способно. Использование такой силы предполагает намерения и расчёт. Поэтому, учитывая наличие как внутренних, так и внешних угроз, путь базового подхода в аналитике информационной войны может опираться на цели существенного изменения картины мира (как об этом писал Почепцов) и «расшифровку» выгодной манипуляторам структуры реальности путём конструирования угроз.Они объясняют враждебные намерения субъекта посредством атрибутивной модели, которая выводит их из нарушений установленных правил и норм.

Изменение картины мира и «навязывание» реципиенту альтернативной его модели есть не что иное, как определённое информационное вторжение. С помощью пропаганды, манипуляций и подобных им элементов, оно стремится подавить морально-политическую способность и личности, и государства защититься от внешних угроз. С учётом сказанного, информационная безопасность понимается нами как состояние защищённости основных национальных интересов личности, общества и государства в информационном пространстве, интересов граждан в обеспечении их потребностей в свободном потоке информации, необходимой для нормальной созидательной деятельности, и достойном образе жизни. Следовательно, не только технические и политические в широком смысле, но и гуманитарные, то есть ориентированные на человека, средства занимают ключевое место в её основании [8, с. 22 ––27].

Среди них процессы социализации, познания как первопричины норм, практики самостоятельного мышления, личностного и государственного конструирования угроз действительно пользуются ныне повышенным спросом. Степень его трансформации в «умную политику» безопасности зависит от уровня ответственности власти. Помимо институциональных инструментов повышения она может получить поддержку со стороны профессиональной этики элиты и аргументации, опирающейся на фундаментальные ценности общества. Политика такой власти способна на ранжирование угроз и на свободу манёвра в их отражении.

Не секрет, что даже при осуществлении этих мер возможны политические манипуляции, искажающие их с целью подмены интересов общества интересами отдельных личностей, групп лиц, кланов, корпораций посредством одностороннего контента, дискурса и пропаганды. Это ведёт к расколу и росту напряжённости в обществе, отрицательно сказывается на его управляемости, так как нарушается система обмена информацией и сигналами между ним

и властью [9, с. 28–29]. Понимание характера и направленности этих угроз, представляющих собой побочный эффект политических действий, ведёт к обнаружению особенностей проявления и конструирования угроз в области информационной безопасности.

Такие угрозы проясняются в процессах политизации и применении «старыми» и «новыми» акторами дискурсов безопасности в борьбе за власть. В результате практически любая ситуация в сфере безопасности становится фокусом множественных трактовок, исходящих из широкого круга объектов безопасности, источников опасности в конкретных её областях. Кроме того, угрозы, понимаемые как риски, характеризуются неопределённостью следствий, что диктует всестороннюю проработанность стратегий обеспечения безопасности, продуманность информационных потоков, преследующих разные цели и направленных на разных адресатов с эффектом развития и личности, и государства. Как никогда, нужна конверсия этой неопределённости в поиск внутренних стимулов развития.

В контексте разворачивающихся вокруг России событий процессы обеспечения информационной безопасности являются сегодня едва ли не самыми насущными. Ибо не столько расширение масштабов санкций, что не исключает их углубления,, сколько рост специальных операций в рамках информационной войны вплоть до некоего политического разрешения ситуации будет неуклонно возрастать. Это позволяет говорить об информационной безопасности как о приоритетной в нынешней обстановке форме национальной реальности. Пребывание в ней наполняет бытие российских граждан смыслом и значимостью, поэтому состояние их защищённости как результат выражается в их информационно-психологической достаточности, состоятельности.

Развитие сфер связи, ИКТ и массовых коммуникаций является общепризнанным индикатором оценки развития информационного общества в РФ. В современных условиях оно является, по сути, ядром идущих преобразований, во многом контролирующим решение проблем в процессе реализации национальных интересов. Различая в информационном обществе внутриполитические и внешнеполитические аспекты, важно подчеркнуть, что поскольку данные уровни подразумевают обсуждение экономических, политических и социальных последствий угроз, формирование основных источников опасности сопряжено с борьбой за власть и в сферах внутренней политики, и в международных отношениях.

Список литературы

1. Бергер П., Лукман Т. 1995. Социальное конструирование реальности. М.: Медиум. С. 92, 103–104, 126–127.
2. Бернейс Э. 2012. Манипуляция общественным мнением: как и почему // Полис: политические исследования. № 4. С. 149.
3. Казаков М.А. 2013. Гуманитарная безопасность как основание внутренней политики современной России // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия Социальные науки. № 1(29). Н. Новгород: Изд-во ННГУ.С. 22–27.
4. Международное право. 2009. Учебник / Отв. ред. А.Н. Вылегжанин. М.: Высшее образование, Юрайт-Издат. С. 792.
5. Почепцов Г.Г. 2000. Информационные войны. М.: «Рефл-бук», К.: «Ваклер».С. 20–23.
6. Путин В.В. 2012. Россия и меняющийся мир // Московские новости. 27 февраля.
7. Соловьёв А.И. 2000. Политология: Политическая теория, политические технологии.М.: Аспект Пресс. С. 134.
8. Цуладзе А.2000. Большая манипулятивная игра. М.: Алгоритм. С. 28–29.

Об авторах

Казаков Михаил Анатольевич – д.полит.н., профессор кафедры прикладной политологии факультета международных отношений ННГУ им.Н.И. Лобачевского. E-mail:kazakov_mihail@list.ru;
Беспалов Дмитрий Николаевич – к.полит.н., доцент кафедры информационной безопасности факультета бизнес-информатики НИУ ВШЭ. E-mail: Dbespalov@hse.ru

INFORMATION WARFARE, THREATS AND INFORMATION SECURITY

D.N.Bespalov, M.A.Kazakov

Higher School of Economics, 101000, Moscow, Myasnitskaya St., 20
Nizhny Novgorod state university, 603950, Nizhny Novgorod, Gagarin Ave., 23

Abstract: *The article presents the opposite, but dependent on each other's reality - Revolutionary War information,information security goals and objectives of their study within the scheme "challenge-response", methodological and analytical support, the role of elites and the information society in promoting information security.*

One of the features of contemporaneityis the global spread of ICT, combined with poor governance and other difficulties in the construction of innovation infrastructures that are based on them in some countries. This leads to the reproduction of threats, primarily related to the ability to use ICT for purposes that are inconsistent with the objectives of maintaining international peace and security, compliance with the principles of non-use of force, non-interference in the internal affairs of states, etc. In this regard, include such terms as "a threat of information warfare", "information terrorism" and so forth.

Information warfare, which stay in the policy declared the struggle for existence, and relationships are defined in terms of "friend-enemy", "ours-foreign". Superiority over the opponent or "capture of its territory" is the aim of political activity. And information security, serving activities similar process of political control, including a set of components, is a technology until their humanitarian.

From the context and the decision itself is the ratio of the achieved results of information and political influence to the target - a positive image of Russia. Bringing its policy in line with the demands of a healthy public opinion provides conductivity of theauthorities initiatives in the country and increases the legitimacy of the Russian Federation actions in the world.

Key words: information warfare, communication, manipulation, propaganda, information security, information society, public opinion, elite.

References

1. Berger P., Lukman T.1995. Social'noe konstruirovanie real'nosti [Social construction of reality]. Moscow, Medium Publ. P. 92, pp. 103–104, 126–127. (In Russian)
2. Berneis E. 2012.Manipulyaciya obschestvennym mneniem: kak i pochemu [Manipulation of the Public Opinion: How and Why] // Polis: Political Research, no.4, p. 149. (In Russian)
3. Kazakov M.A. 2013.Gumanitarnaya bezopasnost' kak osnovanie vnutrennei politiki sovremennoi Rossii [Humanitarian Security as a Base of the Internal Policy of Contemporary Russia]// Vestnik of the University of Nizhniy Novgorod. Social Sciences Series,no.1(29).N. Novgorod, NNGUPubl.P. 22–27. (In Russian)
4. Mezhdunarodnoe pravo [International Law]. Handbook / Ed. By A.N. Vylegzhanin. Moscow, Higher Education: Urait Izdat Publ., 2009. P. 792. (In Russian)
5. Pocheptsov G.G. 2000. Informatsionnye voiny [Information Warfares]. Moscow, Refl Book, K.:Vakler Publ. P. 20–23. (In Russian)
6. Putin V.V. 2012. Rossiya i menyayuschiysya mir [Russia and the Changing World]// Moscow News, 27 Feb. (In Russian)
7. Solovyov A.I. 2000. Politologhiya: politicheskie nauki, politicheskie tehnologhii [Political Science: Political Theory, Political Technologies]. Moscow, Aspekt-Press Publ. P. 134. (In Russian)
8. Tsuladze A. 2000. Bol'shaya manipulyativnaya igra [Big Manipulative Game]. Moscow, Algoritm Publ, P. 28–29. (In Russian)

About the authors

Mikhail Anatol'evich Kazakov – Doctor of Political Sciences, Professor, Department of Applied Political Science of the Faculty of International Relations of the Lobachevsky NNGU. E-mail: kazakov_mihail@list.ru
Dmitriy Nikolaevich Bespalov – Candidate (PhD) of Political Sciences, the Associate Professor of the Department of information security of the Faculty of business informatics of the HSE. E-mail: Dbespalov@hse.ru