

СФЕРА БЕЗОПАСНОСТИ ОБЩЕСТВА: УГРОЗА КИБЕРВОЙНЫ И «СЕТЕВЫЕ ВОЙНЫ»

С.Н. СОКОЛОВА

*Полесский государственный университет,
г. Пинск, Республика Беларусь*

Введение. В представленной статье автор обосновывает существование в современном обществе в эпоху глобализации угрозы кибервойны и «сетевых войн», детерминированных цивилизационными и техногенными причинами. В таком случае общественные отношения претерпевают колоссальные изменения и катастрофически преобразуются, а многомерный потенциал сферы безопасности инсталлирует доминирующие информационные факторы, воздействуя на вектор трансформации общественных отношений.

«Проблема кибервойны крайне злободневна, но плохо «осязается», прежде всего, в понятийном смысле. Может быть поэтому, если судить по отечественной литературе, российская общественность, мягко говоря, плохо осознает эту глобальную опасность» [1, с. 375].

В связи с этим, можно говорить об актуальности информационной безопасности в современном обществе и особенно, если это касается кибервойны и «сетевых войн».

Во-первых, потому что в таком диалектическом контексте информационная безопасность общества представляет собой имиджевый фактор, предопределяющий собой активное преобразование информационно-компьютерных сетей и социального пространства.

Во-вторых, символично, что архитектура безопасности сегодня обязательно включает в себя общественное сознание и предполагает мобилизацию ресурсов для международного сотрудничества, дальнейшего совершенствования стратегии борьбы с международным терроризмом.

В-третьих, кибервойна и «сетевые войны» являются прямым доказательством того, что процесс глобализации многомерен и сложен, так как затрагивает общественные отношения и экономические основы развития современного социума.

Обновленное восприятие реальности под воздействием современных технологий, информационного пространства и постоянное противоборство различных стран приобретает сегодня ярко выраженный характер «сетевых войн». «Принципиальной новацией концепта являлось стирание грани между собственно военной и мирной формой противоборства государств» [2, с. 57].

Угроза кибервойны и «сетевых войн» современными специалистами, политологами и экспертами представлена как объективный процесс происходящих интенсивных изменений, что требует незамедлительного переосмысления основ военной стратегии. «В целом, в современном обществе возникает тенденция, определяемая усилием глубины и масштабности киберпреступлений. Прорисовываются и качественные формы. Сначала элементарные компьютерные преступления. Далее кибертерроризм. И, наконец, высшая форма появления новейшей угрозы существованию человечества – кибервойна» [1, с. 382].

Но, в таком случае, важно уточнить, что в представленной статье, автор целенаправленно акцентирует внимание не только на исследовании сетевых войн, но и на феномене, имеющем отношение к теории войны и к системе безопасности современного общества.

«На рубеже XXI века эта новая дилемма современности начинает материализовываться в необходимость мобилизации ресурсов для международного сотрудничества, дальнейшего совершенствования глобальной стратегии борьбы с международным терроризмом, разработки и использования новых форм и средств защиты прав и свобод человека и гражданина, укрепления демократических устоев общества» [3, С. 104].

Основная часть. Системный подход в изучении сетевых войн не только обозначил новую тактику ведения современной войны, но и видоизменил общую систему координат, что позволяет теоретизировать в рамках качественно обновленного понимания национальной безопасности с учетом решения геополитических вопросов.

«В настоящее время общепризнано, что роль информационной безопасности в системе национальной безопасности существенно возрастает и выходит на первый план» [4, С. 39].

Военная тактика и стратегия, как, впрочем, и вся современная наука, в таком контексте приобретает совершенно иное звучание, подобно тому, как сетевой принцип и методологически грамотно оформленное производство информации априори предопределяет все процессы обмена информацией и преобразует информационное пространство в целом как по форме, так и по содержанию.

Имиджевый фактор имеет большое значение для современного общества и поэтому концентрация внимания на «сетевых войнах» в системе безопасности не случайна, так как сегодня в мире информационная составляющая становится более заметной деструктивной составляющей, постепенно трансформирующей существующую реальность, активно действующую силу, способную переформатировать информационное пространство, изменить историю цивилизации, и может быть, «в силу неконтролируемого и непредсказуемого глобального информационно-компьютерного взаимодействия государств, человечество испытает очередную мировую войну» [1, С. 383].

Новизна авторского взгляда именно в этом и состоит, чтобы предложить не только научные дефиниции для анализа закономерностей развития информационного пространства и взаимосвязей, проявляющихся в процессе реализации современной военной стратегии (медийного, дипломатического, экономического, технического обеспечения безопасности), но и представить онтологическую структурную составляющую, а также представить краткую характеристику этого многогранного явления.

Регулярный и эффективный информационный обмен, являющийся сейчас неотъемлемой частью современной реальности, органично вплетен в динамично развивающиеся общественные отношения и представляет собой постоянно действующий механизм для влияния на социально-политические процессы и формирование общественного сознания, изменения экзистенции человека. Именно поэтому, информационное общество, в котором особая роль и значение принадлежит информации, социальному интеллекту, является сегодня настоящим «полем битвы» и стратегически важным плацдармом в постиндустриальном обществе.

Необходимо осуществлять регулирование сферы безопасности, которое должно быть направлено не только на предотвращение угрозы «сетевых войн», но и на осуществление комплекса мер по укреплению конституционного строя, суверенитета и территориальной целостности российского государства. Речь может идти о создании интегрированной в общественное сознание и долгосрочной перспективной программы развития и целенаправленного воздействия на сферу безопасности современного общества.

Так, внешнеполитический курс Президента России В.В. Путина свидетельствует о расширении интеграции России. На этой основе аналитики сходятся во мнениях, что интеграционные устремления на постсоветском пространстве получают новый импульс, в том числе и информационный, а «противостояние стран Единого экономического пространства с западными державами может приобрести устойчивые черты» [5, С. 2].

Интеграция сетевой деятельности, и особенно в сфере безопасности, создание активно функционирующего информационного обмена предполагает активное разностороннее взаимодействие, а также необходимое воздействие на общественное мнение, обновленное в ходе реализации концепции военной стратегии. В современном обществе основная идея выражается в следующей формуле: взаимосвязь явлений и процессов раскрывается во взаимодействии элементов единой сети, высокопрофессиональной информационно-сетевой деятельности человека. «Представление о человеке как о сверхсложной, многоуровневой и высокоорганизованной системе с точки зрения современной науки является достаточно естественным и очевидным» [6, С. 8].

В связи с этим, важно учитывать смещение акцентов в современной теории войны, связанных с онтологической составляющей реальности. В информационном пространстве в полном объеме осуществляет себя интроекция в рамках системно-кибернетического подхода, что обусловлено итеративностью, результатами информационно-коммуникативной деятельности различных субъектов (актеров) безопасности. Например, социальные сети, как правило, способствуют высокоэффективной реализации социальных коммуникаций и активно инициируют развитие базовых потребностей.

Основной замысел «сетевых войн» раскрывается в процессе создания информационно-сетевого, коммуникационного механизма, обеспечивающего высокоэффективные системные связи в информационном пространстве, что подразумевает реализацию действенных концептуально стратегически выверенных военных моделей, высокоэффективных сетевых войн, способных то-

тально и в глобальных масштабах оказывать воздействие на процессы демократизации, человека и современное общество в целом.

Следовательно, для современного общества жизненно необходим прогрессивный процесс демократического развития, который «позволит воздействовать на детерминированный хаос и динамику самоорганизации социально–экономических систем» [7, С. 18].

Структурные характеристики сетевых войн предполагают имманентизацию конкретных действий, направленных на формирование программ (моделей) поведения человека в различных ситуациях, например, финансово–экономического кризиса, локальной войны, периода мирного существования различных государств. В таком случае, доминирующая идея сетевых войн заключается в непрекращающемся воздействии на человека и общество ангажированной информационно–сетевой деятельности для осуществления запрограммированного управления в глобальном масштабе.

Существует три основополагающих варианта сценария развития информационно–сетевой деятельности: во–первых, постоянное инициирование искусственного увеличения потребности в использовании информационного пространства, одновременного прекращения к доступу качественной информации; во–вторых, максимальное обеспечение достаточно широкого доступа к информации через сетевые механизмы и инструменты обратной связи, надежно защитив их от внедрения нежелательных субъектов (акторов); и, в–третьих, сокращение до минимума собственной потребности в достоверной информации через обеспечение доступа к широкому спектру оперативного и динамичного информирования.

Следовательно, по своему содержанию сетевые войны можно охарактеризовать следующим образом: всеобщая информационно–адаптированная осведомленность, ценности безопасности, скорость распространения информации, распределение силы (от реализации линейной – к более активной точечной инициативе в информационном пространстве), функциональный контроль над доминирующими стратегически элементами, демассификация, тотальное информационное проникновение.

Сегодня считается, что безопасность – это явление, включающее в себя такие ценности, как «национальная и семейная безопасность, мир во всем мире, общественный порядок, вежливость, уважение к старшим, здоровье, социальная справедливость, уважение традиций, благополучие» [8, С. 8].

Система воздействия на современное общество и его сферу безопасности связана с необходимостью формирования национальных ценностей и, особенно, ценностей безопасности.

Есть еще один определяющий момент, связанный с осознанием необходимости последовательного, активного формирования ценностей безопасности. Как показывает практика, «ценности политической элиты в значительной степени могут отличаться от ценностей большинства граждан» [9, С. 18], что, безусловно, усложняет поиск оптимальных моделей вмешательства государства в общественное бытие.

Конечно, с такими предложениями можно соглашаться, полагая, что отмеченные выше гуманистические установки являются императивами сферы безопасности, и поэтому в процессе регулирования их следует внедрять в общественное сознание. Однако при этом следует иметь в виду, что данные положения фактически нивелируют многие полезные отличительные черты рынка (конкуренция) и демократических преобразований (при которых не абстрактное равенство становится основой действий в сфере безопасности, а четко сформулированные национальные интересы и ценности). При этом надо понимать, что такое философско–ценностное наполнение сферы безопасности может быть расценено как конфликтогенное, субъективное и релятивное. Но это не должно отталкивать, потому что социальный гуманизм применительно к государственному регулированию – это целенаправленность, организованность и результативность деятельности по реализации целей демократического развития, а не следование абстрактным ценностям. Будет вполне целесообразным внедрить в государственное регулирование сферы безопасности такие ценности как прагматизм и нацеленность на обязательное достижение запланированного результата (в рамках национальных интересов). Такое требование будет соответствовать базовым ценностным категориям, сложившимся в мировой практике обеспечения безопасности. Национальные ценности в системе национальной безопасности играют важную роль и определяющее значение, что актуализирует необходимость их продуцирования, обязательного и последовательного внедрения в общественное сознание.

Заключение. Таким образом, взаимосвязанной с вопросами обеспечения демократического развития и формированием соответствующих ценностей является проблема сетевых войн, эффек-

тивного политического лидерства и эффективной политической элиты, способной противостоять деструктивному информационному воздействию на общественное сознание российских граждан. Например, в современной России решение этой проблемы является весьма перспективным для системы государственного регулирования, как, впрочем, и для сферы безопасности. Влияние государства на сферу безопасности, как и в большинстве государств мира, в большей степени будет принимать характер информационно–сетевой деятельности («сетевые войны» и «кибервойны»).

В связи с этим, возникает вопрос: «В чем же главная опасность сетевых войн для российской государственности? Во–первых, лежащая в их основе война идей ведет к разрушению базовых ценностей народа и государства, национальной, конфессиональной и культурной идентичности.

Во–вторых, информационный и идеологический вакуум ограничивает стратегический выбор страны в глобализирующемся мире и «делает ее частью системы планетарного контроля» [10, С. 96].

Резюмируя, поясню, что современный социум носит преимущественно информационный характер, а кибервойна и «сетевые войны» являются неотъемлемой частью общественных отношений в обществе сегодня и в ближайшем будущем.

ЛИТЕРАТУРА

1. Еляков, А.Д. Кибервойна – новейшая угроза обществу в XXI веке? /А.Д. Еляков // Безопасность Евразии. – № 1(39)–2010. – С. 375–383.
2. Багдасарян, В.Э. Новые технологии борьбы с российской государственностью / В.Э. Багдасарян // Национальная безопасность: научное и государственное управленческое содержание: материалы Всероссийской научной конференции. – Центр пробл. анал. и гос.–упр., Проект. – М.: Научный эксперт, 2010. – С. 55–72.
3. Зонов, Ф.А. Международный терроризм и мировой опыт борьбы с ним / Ф.А. Зонов // Власть. – 2011. – № 12. – С. 103–106.
4. Дербин, Е.А. Вызовы и угрозы национальной безопасности Российской Федерации в информационной сфере / Е.А. Дербин // Национальная безопасность: научное и государственное управленческое содержание: материалы Всероссийской научной конференции. – Центр пробл. анал. и гос.–упр., Проект. – М.: Научный эксперт, 2010. С. 38–55.
5. Осипов, М. Интеграционное будущее / М. Осипов // Народная газета, 8 мая, 2012 г.
6. Лебедев, С.А. Многомерный человек: онтология и методология исследования / С.А. Лебедев, Ф.В. Лазарев. – М.: Издательство Московского университета, 2010. – 96 с.
7. Поздняков, А. Порядок и хаос в динамике социально–экономических систем / А. Поздняков // Наука и инновации. – 2011. – № 12 (106). – С. 13–18.
8. Степанянц, М.Т. Культура как гарант российской безопасности / М.Т. Степанянц // Вопросы философии. – 2012. – № 1. – С. 3–13.
9. Смирнов, Д.С. Ценностные ориентации политической элиты как фактор ее эффективности / Д.С. Смирнов // Власть. – 2007. – № 2. – С. 18–24.
10. Орлов, И.Б. Сетевые войны – угроза национальной безопасности России / И.Б. Орлов // Национальная безопасность: научное и государственное управленческое содержание: материалы Всероссийской научной конференции. – Центр пробл. анал. и гос.–упр., Проект. – М.: Научный эксперт, 2010. – С. 86–96.

THE SECURITY SPHERE OF SOCIETY: CYBERWAR THREAT AND «NETWORK WARS»

S.N. SOKOLOVA

Summary

In article the author focuses on the threat of cyber war and «network wars». Regular and effective exchange of information organically woven into the dynamic public relations and it is a permanent mechanism for active influence on public consciousness and influence on the socio– political processes. Today the post–industrial society is a strategically important springboard for the implementation of social programs and policies, because information and computer technology

© Соколова С.Н.

Поступила в редакцию 18 марта 2014г.