УДК 070 (079)

ИНФОРМАЦИОННЫЕ ВОЙНЫ КАК ЗОНТИЧНЫЙ КОНЦЕПТ СОВРЕМЕННОГО МАСС-МЕДИЙНОГО ПРОСТРАНСТВА

Качмазова З.Н.

Ростовский государственный экономический университет, Ростов-на-Дону, e-mail: valentina-kihtan@yandex.ru

Сегодня развитие информационных технологий выступает не только двигателем научно-технического процесса, но может быть использовано и уже применяется различными силами в качестве мощного оружия разрушения. За последние два десятилетия информационные и коммуникативные технологии – в наступательных или оборонительных целях – все чаще задействуются в сценариях информационных войн (ИВ). Можно с уверенностью говорить о том, что текущее столетие внесло некоторые исключительные измерения в искусство ИВ. В связи с этим традиционные понятия об основаниях превосходства и динамике силового воздействия, обнаруживающиеся между агрессорами и атакуемой стороной, настоятельно требуют пересмотра. ИВ предстают не только имманентной частью «войны четвертого поколения», но и эффективным способом изменения сознания общества посредством воздействия на культурные, социальные и идеологические ценности. В рамках данной статьи ИВ исследуются как зонтичный концепт, анализируются основные концепции данного типа войн. ИВ представляют собой всеобъемлющий концепт, который настоятельно требует от всех государств последовательных и синхронизированных действий по контролю информационного пространства.

Ключевые слова: информационные войны, пропаганда, информационные системы и инфраструктуры, зонтичный концепт

INFORMATION WARFARE AS AN UMBRELLA CONCEPT OF CONTEMPORARY MASS MEDIA SPACE

Kachmazova Z.N.

Rostov State Economic University, Rostov-on-Don, e-mail: valentina-kihtan@yandex.ru

Today, the development of information technology is not only the engine of scientific and technical process, but can be used and is already being used by various forces as a powerful weapon of destruction. For the latest two decades information and communication technologies with offensive or defensive aims have been often used in information warfare scenarios. We may argue that the current century has formed some exclusive dimensions on the level of Information Warfare (IW) arts. That is why some traditional notions on the base of advantage and dynamics of force impact between aggressors and the side attacked require to be reconsidered. IW is not only the immanent part of fourth generation wars, but also an effective way of changing the society consciousness by impacting on cultural, social and ideological values. In this article IW is investigated as an umbrella concept, the basic conceptions of this kind of war are analyzed. Information war constitute a comprehensive concept, which urges all States consistent and synchronized action for control of information space.

Keywords: information warfare, propaganda, information systems and infrastructures, umbrella concept

Одной из действенных технологий, которые задействуются в ИВ, являются пропагандистские кампании, предполагающие априорно запланированный характер распространения новостей, особые аргументы, призывы к воздействию на мировоззрение и деятельность некоторой группы людей. В 1990-х гг. историк Оливер Томпсон определил широкое понимание пропаганды, которая включает в себя как умышленные, так и ненамеренные способы модификации поведения, описываемые как «использование разного рода коммуникативных умений для внедрения действенных изменений в установках и поведении представителей некоторой группы людей» [12, с. 488].

Правительства и корпоративный сектор способен прибегать к ИВ как в оборонительных, так и наступательных целях в рамках физических и виртуальных доменов. ИВ пренебрегают границами государств, уровнем образования людей, их культурными воззрениями. Они дают возможность реализовывать как прямые, так и неявные атаки с любой точки мира в течение нескольких секунд. Этому, в частности, способствует применение тонковолокнистой оптики, спутников, лазерных средств коммуникации, кабельного телевидения, мобильных телефонов и других технологических достижений, благодаря которым информация мгновенно поступает в любую точку планеты.

Информационная революция породила новые способы развязывания и ведения войн, которые по своей сути оказываются в большей степени подрывными, нежели деструктивными. В связи с этим государства, которые активно поддерживают технический прогресс, априорно призваны налагать на себя этические обязательства по сдерживанию негативных последствий прогресса, связанных с совершенствованием ИВ.

Понятие «ИВ» не обладает универсальным определением [2, с. 23; 3, с. 51]. Как представляется, наиболее упрощенным

предстает определение ИВ как «особой способности эксплуатировать информационную систему противника в своих целях, подрывать ее, сознательно вводить противника в заблуждение, при этом одновременно оберегать свою информационную систему от внешнего воздействия» [13, с. 7]. В рамках данной публикации мы предлагаем следующее рабочее определение ИВ: это синхронизированное сочетание физических и виртуальных действий, направленных на конкретные страны, организации или индивидов с целью реализации своих целей и одновременное предотвращение аналогичных попыток со стороны противника. При развязывании ИВ – серии мер, направленных на достижение значительного превосходства, победы над противником – мишенью может стать как население отдельно взятой страны, так и особая политическая, религиозная или этническая группа, диктатор страны.

Технология ИВ активно задействовалась еще древними греками. Единственная разница между примерами из истории и современным состоянием проблемы заключается в технологических особенностях [1, с. 488].

На современном этапе развития ИВ представляют собой зонтичный концепт, который по своему определению охватывает разрозненные положения из многих сфер знания и формирует из них более сложное образование, обладающее действенной объяснительной силой. Среди наиболее частотных терминов, которые используются для обозначения разнообразных практик в аспекте ИВ, можно отметить следующие: безопасность информационных систем, информационное превосходство, информационное доминирование, защита критической инфраструктуры, операционная безопасность и многие др.

ИВ становятся все более изощренными и действенными вследствие интенсивного развития сектора информационных технологий. Негативное влияние ИВ на самые разнообразные ценности – как и само сознание – испытывающей воздействие стороной может не ощущаться в течение длительного периода, а иногда так и остается незамеченным. Сторона, прибегнувшая к ИВ, способна обнаружить для своих действий соответствующий канал вследствие взаимосвязанности и взаимозависимости многих инфраструктур в современном мире.

Подавляющее большинство современных национальных государств выражают согласие с установкой, выраженной американскими военными кругами, согласно которой усиленные информационные действия охватывают весь спектр возникающих в мире конфликтов, начиная фазой разворачивания военных действий и заканчивая моментом заключения перемирия. Факт инициации подобных войн сам по себе априорно порождает конфликт. Согласно Е.А. Эрикссону, ИВ – наряду с ядерным, химическим и биологическим вооружением – рассматриваются в качестве потенциального оружия массового поражения или, по крайней мере, разобщения масс [9].

Чтобы понять истинную природу ИВ приведем мнения некоторых известных западных политиков и исследователей на обсуждаемую нами проблему. В частности, М. Либецки в эссе «Что собой представляют информационные войны?» указывает, что семь форм данной разновидности войн конкурируют между собой за позицию центральной метафоры в процессе информационного воздействия: войны, навязываемые с целью контроля; войны, разворачиваемые разведывательными спецслужбами; электронные войны; психологические войны; войны хакеров; войны за право обладания экономической информацией; войны, которые ведутся в кибер-пространстве [9].

Согласно точке зрения В. Швартау, «ИВ – это прежде всего использование информации и информационных систем как наступательного, так и оборонительного механизма (орудия) против противника» [9]. Данный исследователь распределяет ИВ на три основных класса:

1) войны, направленные на неприкосновенность частной информации;

2) корпоративный шпионаж;

3) глобальные войны, носящие террористический характер.

В одном из своих исследований В. Швартау приводит такое определение ИВ: это действия, предпринимаемые с целью сохранения целостности своих информационных систем, их защита от внешней эксплуатации, коррумпирования или разрушения и в то же время эксплуатация, коррумпирование или разрушение информационных систем противника, а также достижение информационного превосходства в процессе применения силы [9].

Командующий 23-м эскадроном информационных действий при американских воздушных силах лейтенант-полковник Г. Рэттрей полагает, что главной частью войн XXI века станут стратегические операции в кибер-пространстве. Войны в кибер-пространстве должны фокусироваться не столько на использовании актуальной информации, сколько на ИВ как средстве достижения целей посредством «цифровых» атак на центры тяжести противника [8, с. 14]. В указанном контексте политик

сосредотачивается на организационных структурах и средствах, необходимых для эффективного совершения компьютерных атак, которые способны разрушить информационные инфраструктуры противника. На стратегическом уровне ИВ одновременно представляют собой и возможность, и угрозу [10, с. 190–191].

«Словарь военной и сопутствующей военному делу терминологии» дает следующее определение ИВ: это «информационные операции, проводимые во время кризиса или конфликта с целью достижения или продвижения специфических целей в отношении специфического противника или противников. Цель ИВ – контроль или оказание влияния на действия тех людей, которые принимают решения. Сфера контроля может подвергаться прямой манипуляции; сфера влияния – только неявной манипуляции. Контроль и влияние являются сутью власти» [11, с. 10].

Исследователи также прослеживают сравнение между информационными и конвенциональными войнами. Так, Р. Эйер пишет, что указанные типы войн предстают, по своей сути, разными явлениями, предполагают различные коннотации, преследуют не менее различные цели. В конвенциональных войнах имеет место визуальное поле сражения, вокруг которого организуются противоборствующие военные силы. ИВ, напротив, не обладают физическим пространством сражения, это логическое поле битвы [5]. В конвенциональных войнах противники явно идентифицируются, на мобилизацию сил требуется определенное время; в ИВ униформа отсутствует, мобилизация сил не требуется, война начинается элементарным нажатием кнопки [7].

Дж. Арквила и Д. Ронфелд определяют ИВ несколько в ином ключе: «Информационная революция станет причиной сдвигов как в характере вступления разных обществ в конфликт, так и в том, как вооруженные силы противоборствующих сторон развяжут войну. Мы предлагаем разграничивать «сетевую войну», основой которой являются конфликты, порождаемые информационными процессами, и «кибер-войну», развязываемую на уровне военных сил» [4, с. 141].

Проблемы ИВ интенсивно разрабатываются китайскими исследователями. В частности, Ш. Вейгнанг, который традиционно считается «отцом китайских ИВ» выдвигает концепцию, которая в некотором отношении отличается от взглядов американских экспертов. ИВ означают войну в самом прямом смысле, а не способ ведения соответствующих действий, как это понимают американские эксперты. ИВ предстают конкретной моделью ведения войны, а не моделью целенаправленных действий [6, с. 684-686]. В условиях ИВ противоборствующие стороны конкурируют за информационное пространство и доминирование над источниками информации. Суть ИВ заключается в том, чтобы – посредством информационного превосходства – вынудить «врага» сдаться без вступления в военные действия [6, с. 685]. При этом ИВ не ограничиваются периодами конфликтов и кризиса, это непрекращающийся процесс.

В современной китайской традиции войны классифицируются по двум типам:

1) «вероломные», которые происходят непосредственно на поле сражений и, как правило, являются ограниченными по масштабам и во времени;

2) «сдерживающие», которые охватывают все географическое и темпоральное пространство, не задействованное «вероломными войнами»; противоборствующие стороны обращают свою силу в информационное воздействие на противника и стремление сдержать его вооруженные действия. Подобная перспектива ведет к ИВ в целом ряде регионов как отчаянным попыткам сфокусироваться на том, чтобы остановить натиск противника, подорвать его «воинствующую» деятельность. Таким образом, ИВ – это сражения с разной степенью интенсивности, которые ведутся сразу на нескольких фронтах [6, с. 686]. ИВ реализуют прежде всего оборонительные действия от внешнего военного и информационного воздействия.

Таким образом, ИВ представляют собой сложный концепт. Будучи зонтичным термином, они играют решительную роль на:

1) операционном уровне: посредством компьютеров, соответствующего программного обеспечения, интернета одна из сторон способна взять в свои руки контроль над инфраструктурой противника, повысив эффективность, скорость своих соответствующих действий, опередив противника в освещении текущих событий;

2) стратегическом уровне: ИВ задействуются на всем пространстве государства-мишени в течение длительного времени с учетом всех доступных механизмов, включая пропаганду, психологические атаки внутри государства, а также – через дипломатические круги – во всем мире.

Печатные и электронные СМИ становятся одним из наиболее эффективных способов распространения избранной информации против государства-мишени через восприятие этой информации читающей аудиторией. ИВ являются существенным компонентом текущих военных операций,

их прагматическое действие нацелено на формирование потенциальной стратегической уязвимости инфраструктур государства-мишени. В настоящее время ИВ представляют собой серьезную угрозу для мира, поскольку в процессе их проектирования задействуются последние научные и технические достижения, которые умело сочетаются со значительными изменениями в искусстве ведения войны. В связи с этим по силе разрушительных последствий ИВ можно сравнить с созданием ядерного оружия в середине 1940-х гг. Российская Федерация воспринимает данную угрозу настолько серьезно, что предложила ООН запустить проект по созданию договора о запрещении ИВ, признавая, что их деструктивный потенциал соизмерим со стратегическим ядерным оружием.

Полагаем, что в настоящее время нельзя еще говорить о быстром и легком решении такой проблемы, как угроза ИВ. Даже самые передовые государства мира проявляют неспособность реагирования на информационные атаки. ИВ представляют собой глобальную угрозу, поэтому их проблема настоятельно требует глобального разрешения. ИВ представляют собой всеобъемлющий концепт, который настоятельно требует от всех государств последовательных и синхронизированных действий по контролю информационного пространства.

Список литературы

1. Волковский Н.Л. Журналистика в информационных войнах: исторические истоки и современные тенденции: дис. … д-ра филол. наук. – СПб., 2003. – 641 с.

2. Михальченко И.А. Информационные войны и конфликты идеологий в условиях геополитических изменений конца XX века: дис. … полит. наук. – СПб., 1998. – 210 с.

3. Соколова А.М. Информационные войны в условиях глобализации: социально-политический анализ: дис. … канд. философ. наук. – Красноярск, 2007. – 174 с.

4. Arquilla, J., Ronfeldt, D. The Advent of Netwar. – Santa Monica, CA: Rand Corporation, 1996. – 245 p.

5. Ayers R. The New Threat: Information Warfare // The RUSI Journal. – 1999. – № 5. – P. 23–27.

6. Barrington M., Barrett Jr. Information Warfare: China's Response to U.S. Technological Advantages // International Journal of Intelligence and Counter Intelligence. – 2005. – № 4. – P. 684–686 // http://dx.doi.org/10.1080/08850600500177135.

7. Blank S.J. Nuclear Strategy and Nuclear Proliferation in Russian Strategy // Report of the Commission to Assess the ballistic Missile Threat to the United States. – W., 2001. – 35 p.

8. Blaise C. Review of the «Strategic Warfare in Cyberspace», by Gregory J. Rattray // The Information Society: An International Journal. – 2003. – № 4. – P. 11–19.

9. Eriksson E.A. Viewpoint: Information Warfare: Hype or Reality? // The Nonprolioferation Review. – 1999. – № 3 // http://dx.doi.org/10.1080/ 10736709908436765.

10. Grenier J. Strategic Warfare in Cyberspace // Technology and Culture. – 2003. – № 1. – P. 187–203.

11. Kovacich J., Luzwick J. Everything You Want to Know about Information Warfare but Were Afraid to Ask // Information Systems Security. – 1999. – № 4. – P. 9–20.

12. Rathmell A. Information Warfare and Sub-State Actors: An Organizational Approach // Information, Communication & Society. – 1998. – № 4. – P. 483–492 // http://dx.doi.org/10.1080/13691189809358984.

13. Stephenson P. Information Warfare, or Help! The Sky is Falling // Information Systems Security. – 1999. – № 1. – P. 6–10.

References

1. Volkovsky N.L. Journalism in the information wars: the historical roots and contemporarytrends: a thesis of doctor of philological Sciences, St. Petersburg, 2003. 641 p.

2. Mikhalchenko I.A. the Information war in the geopolitical changes of the late twentieth century: Diss. political Sciences.

3. Sokolova A.M. the Information war in the conditions of globalization: the socio-political analysis. dissertation of candidate of philosophical Sciences, Krasnoyarsk, 2007 174 p.

4. Arquilla, J., Ronfeldt, D. The Advent of Netwar. – Santa Monica, CA: Rand Corporation, 1996. 245 p.

5. Ayers R. The New Threat: Information Warfare // The RUSI Journal. 1999. no. 5. pp. 23–27.

6. Barrington M., Barrett Jr. Information Warfare: China's Response to U.S. Technological Advantages // International Journal of Intelligence and Counter Intelligence. 2005. no. 4. pp. 684–686 // http://dx.doi.org/10.1080/08850600500177135.

7. Blank S.J. Nuclear Strategy and Nuclear Proliferation in Russian Strategy // Report of the Commission to Assess the ballistic Missile Threat to the United States. W., 2001. 35 p.

8. Blaise C. Review of the «Strategic Warfare in Cyberspace», by Gregory J. Rattray // The Information Society: An International Journal. 2003. no. 4. pp. 11-19.

9. Eriksson E.A. Viewpoint: Information Warfare: Hype or Reality? // The Nonprolioferation Review. 1999. no. 3 // http://dx.doi.org/10.1080/ 10736709908436765.

10. Grenier J. Strategic Warfare in Cyberspace // Technology and Culture. 2003. no. 1. pp. 187–203.

11. Kovacich J., Luzwick J. Everything You Want to Know about Information Warfare but Were Afraid to Ask // Information Systems Security. 1999. no. 4. pp. 9–20.

12. Rathmell A. Information Warfare and Sub-State Actors: An Organizational Approach // Information, Communication & Society. 1998. no. 4. pp. 483–492 // http://dx.doi.org/10.1080/13691189809358984.

13. Stephenson P. Information Warfare, or Help! The Sky is Falling // Information Systems Security. 1999. no. 1. pp. 6–10.

Рецензенты:

Кудряшов И.А., д.фил.н., профессор кафедры русского языка и теории языка, ФГАОУ ВПО «Южный федеральный университет», г. Ростов-на-Дону;

Клемёнова Е.Н., д.фил.н., профессор кафедры журналистики, Ростовский государственный экономический университет (РИНХ), г. Ростов-на-Дону.

Работа поступила в редакцию 18.04.2014.