УДК 355.015

В.Г. Шур[1]

ИНФОРМАЦИОННОЕ ОРУЖИЕ КАК СРЕДСТВО ГИБРИДНОЙ ВОЙНЫ

V.G. Shur

INFORMATION WEAPONS AS A MEANS OF HYBRID WAR

Динамизм, сложность и противоречивость происходящих изменений в мире в начале XXI в. требуют объективного анализа создавшейся ситуации для принятия адекватных мер по обеспечению национальной безопасности. На современном этапе борьбы за сферы влияния на смену чисто силовым методам постепенно приходят более гибкие средства, составной частью которых являются контроль и управление информационными ресурсами государства. Информация превратилась в глобальный, принципиально неистощимый ресурс человечества, вступившего в новую эпоху интенсивного освоения информационного пространства. В свою очередь, повышение роли информационных кибернетических систем в жизни общества заставляет ведущие государства мира создавать эффективные инструменты информационного воздействия. В этой связи особый интерес представляет феномен гибридных войн (англ. hybrid warfare), военная стратегия, по некоторым взглядам, объединяющая в единое целое обычную войну, малую войну и кибервойну. Термин «гибридная война» зачастую используется для обозначения согласованного применения политико-дипломатических, информационно-психологических, экономических и силовых средств для достижения стратегических целей (Defence lacks doctrine to guide it through cyberwarfare (http://www.nextgov/ng20100913). В правительственных кругах и аналитических сообществах иностранных государств широко употребляются такие определения, как «неявные военные действия», «нелинейные», «ассиметричные», «нетрадиционные» и «гибридные» операции [1]. Наконец, в редакторском предисловии справочника Military Balance 2015 «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;

– экономическое давление [2].

Следовательно, мы можем рассматривать информационно-психологические операции как составную часть гибридной войны, а информационное оружие – как средство осуществления подобной деятельности.

Информационное оружие – это специально подобранная информация, используемая для целенаправленного воздействия на политическую, экономическую, военную и иные сферы жизнедеятельности того или иного государства, а также средства и способы ее доведения до адресата. Основными объектами его воздействия можно считать информационно-технические и социальные системы.

Применение информационного оружия имеет давнюю историю. Имеется множество примеров, когда сам факт передачи ложной или искаженной информации оказывал существенное влияние на принятие решений в ходе боевых действий. В истории зафиксированы факты успешного использования таких приемов, как перевоплощение, угрозы, ложные переговоры, дезинформация и т.д. Описания случаев рефлексивного управления можно найти в древних надписях Египта, Ассирии, Греции, древнекитайском военном трактате Сунь-цзы и комментариях к ним. В общем случае цель такого воздействия состояла и состоит в том, чтобы, передавая информацию, изменить замыслы противника по

[1] Кандидат исторических наук, доцент АНО ВО «Российский новый университет».

проведению стратегической или тактической операции в нужном другой стороне направлении. К относительно современным примерам квалифицированного информационного воздействия можно отнести американские коммуникационные акции по дезинформации иракского руководства во время войны в Персидском заливе.

Другой тип информационного оружия – широко или узко ориентированное информационно-психологическое воздействие, способное инициировать деструктивные общественные процессы. Разрушительные последствия его применения, подкрепленного мощью современных СМИ, были очевидны в период холодной войны (особенно на ее заключительном этапе). Актуальны они и в настоящее время в условиях международных, национальных и локальных конфликтов различной степени интенсивности.

Еще в середине 90-х годов прошлого столетия появились сообщения о так называемом вирусе V666, который обладает способностью избирательного воздействия на психологическое состояние пользователя компьютера. По сообщениям экспертов, опубликованных в западной прессе, вирус выдает на экран особую цветовую комбинацию, погружающую человека в своеобразный гипнотический транс и вызывающую у него такое подсознательное восприятие, которое резко изменяет функционирование сердечно-сосудистой системы вплоть до блокирования сосудов головного мозга, что в ряде случаев может привести к летальному исходу [3].

Помимо этого, обязательными видами информационного оружия являются радиоэлектронная борьба, радиопротиводействие и радиоперехват, существенно влияющие на эффективность разведки, связи и управления на поле боя, а также постановка и подавление помех действию традиционного и новейшего высокоточного оружия, использующего различные виды излучения. Отражение электромагнитных, акустических и инфракрасных сигналов радиоэлектронного подавления (РЭП) осуществляется автоматически наземными, корабельными и авиационными системами постановки помех. Широкомасштабное применение РЭП было не раз продемонстрировано в ходе операции «Буря в пустыне» в Персидском заливе, боевых действий против формирований ИГИЛ на Ближнем Востоке.

Целью применения информационного оружия, по взглядам военно-политического руководства США, является завоевание информационного превосходства над противником и нанесение ему информационного поражения. При этом используются принципы внезапности, многоканальности, скрытности, комплексности, систематичности и целостности.

С помощью информационного оружия могут решаться следующие задачи: нанесение серьезного ущерба жизненно важным интересам государства в политической, экономической, оборонной и других сферах деятельности; подрыв международного авторитета государства; затруднение принятия решения органами управления; создание атмосферы напряженности и нестабильности в обществе; дискредитация органов власти и управления; провоцирование социальных, политических национальных и религиозных беспорядков; инициирование забастовок, массовых выступлений и других акций протеста; нарушение функционирования системы управления войсками, различными объектами оборонного значения; создание атмосферы бездуховности и безнравственности, негативного отношения к культурному наследию, а также ряд других. Реализация вышеуказанных задач может нанести противостоящей стороне существенный материальный и моральный ущерб, вызвать у населения неадекватное социальное или криминальное поведение, оказать негативное влияние на процессы образования, культуры и формирования личности.

Американские эксперты выделяют следующие атакующие средства информационного воздействия, ряд из которых довольно давно известен, другие – сравнительно недавно.

1. Компьютерные вирусы, представляющие собой специальные программы, внедряемые в «нужную электронную среду». Они способны передаваться по линиям связи и сетям обмена информацией, проникать в системы управления. При этом они способны заполнить всю память компьютера-жертвы другими данными и, в конечном счете, блокировать его.

2. Логическими бомбами, как известно, называют программные закладные устройства, заранее внедренные в информационно-управляющие центры военной и гражданской инфраструктуры, которые по сигналу или в установленное время приводятся в действие, уничтожая, искажая или дезорганизуя работу программно-технических средств.

3. Средства подавления информационного обмена в коммуникационных сетях, его фальсификации, передачи по каналам государственного и военного управления, а также по каналам СМИ нужной (с позиции противодействующей стороны) информации.

4. Способы и средства, позволяющие внедрить компьютерные вирусы и логические бомбы

в государственные и корпоративные информационные системы и управлять ими.

Информационное оружие применяется в различных сферах деятельности государства.

В частности в политической сфере с помощью информационного оружия могут решаться следующие задачи: манипулирование общественным сознанием и политической ориентацией социальных групп населения страны с целью создания политической напряженности и хаоса; снижение уровня информационного обеспечения органов власти и управления, что может привести к принятию ошибочных управленческих решений и, как следствие, к негативному отношению народа к властным структурам; дестабилизация политического взаимодействия между партиями, объединениями и движениями с целью провоцирования конфликтов, разжигания недоверия, подозрений, обострения политической борьбы; дезинформация населения о работе государственных органов, подрыв их авторитета, разрушение структур и систем формирования общественного мнения, включая процесс выявления, изучения, анализа и интерпретации событий и фактов; информационная поддержка агентов влияния, способствующих дезорганизации политических, экономических, социальных, духовных, военных и других структур.

В экономической области информационному воздействию могут быть подвержены такие компоненты, как информационная система государственной статистики; коммерческая информация хозяйственных субъектов всех форм собственности; биржевая, налоговая, таможенная, внешнеэкономическая информация.

В сфере обороны наиболее уязвимыми считаются следующие элементы: информационные ресурсы аппарата военного управления, научно-исследовательских учреждений, содержащие сведения и данные об оперативных и стратегических планах подготовки и ведения боевых действий, о составе и дислокации войск, о мобилизационной готовности, тактико-технических характеристиках вооружения и военной техники; информационные ресурсы предприятий оборонного комплекса, содержащие сведения о научно-техническом и творческом потенциале, объемах поставок и запасах военной техники, их боевых возможностях и проводимых в интересах обороны фундаментальных и прикладных научно-исследовательских работах; системы связи и управления войсками и оружием, их информационное обеспечение; морально-психологическое состояние войск; информационная инфраструктура, в том числе центры обработки и анализа информации, пункты управления, узлы и линии связи [4].

Таким образом, информационное оружие может служить средством уничтожения, искажения или хищения информационных массивов, добывания разведывательной информации после преодоления систем защиты, ограничения или воспрещения доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей и компьютерных систем, а также всего высокотехнологического обеспечения жизнедеятельности общества и функционирования государства.

В условиях применения информационного оружия необходимо учитывать воздействие с помощью определенной информации, оказываемое противником. При этом выделяется информационное воздействие на управляющую систему и объект управления.

Основными показателями и критериями эффективности применения информационного оружия следует считать изменение функционирования систем управления противника в соответствии с запланированным алгоритмом воздействия. Спецификой его применения в боевых условиях на нынешнем этапе развития информационных технологий является воздействие не только на субъекты управления, но и на нижний уровень управленческой структуры вплоть до отдельного индивида, поскольку негативное воздействие на непосредственную информационную среду, окружающую каждого солдата противника, создает предпосылки для достижения победы.

Возвращаясь к гибридной войне как комбинации различных элементов, отметим, что подобная война может быть развернута на всех возможных направлениях, в том числе и информационном. По мнению Г.Г. Почепцова, «это одновременно экономическая, репутационная, смысловая, человеческая…война. На нее должны работать все, кто имеет влияние на население: актеры, певцы, писатели, режиссеры. Военные действия задают лишь фон для более масштабной войны в человеческом разуме. Это скорее гуманитарная война, в которой военные действия являются второстепенными. Когда мы в первую очередь обращаем внимание на них, мы делаем ошибку» [5]. При некоторой спорности данного заявления, широта подхода ученого-коммуникативиста заслуживает внимания.

Исходя из вышеизложенного можно сделать следующие выводы. Создание и развитие новых видов информационно-психологического

оружия отражает тенденцию перехода от войн индустриальной эпохи, имевших своей целью физическое уничтожение противника, к войнам эры информатики, когда можно добиться победы без единого выстрела. Следует также отметить, что в современных условиях наряду с огневым и экологическим воздействием на противника возрастает значение информационно-психологического воздействия. Проводимые информационные операции могут быть настолько эффективными, что ведение полномасштабных боевых действий становится менее значимым.

Литература

1. Клименко С. Теория и практика ведения «гибридных войн» // Зарубежное военное обозрение. – 2015. – № 5. – С. 109–112.

2. The Military Balance 2015 IISS. – 2015. – 11 February Editor's Introduction. – P. 5–8.

3. Абдеев Р. Философия информационной цивилизации. – М., 1994. – С. 7.

4. Информационный сборник «Безопасность». – 2006. – № 1. – С. 53–59.

5. http://psyfactor.org/psyops/hybridwar5.htm