УДК 94(4/9)

[1]Е.М. Ужкенов, [2]Т.М. Есназаров*

[1]КазУМОиМЯ имени Абылай хана, к. и. н., доцент, Республика Казахстан, г. Алматы
[2]КазУМОиМЯ имени Абылай хана, магистрант, Республика Казахстан, г. Алматы
*E-mail: yesnazarov. timur@gmail. com

Характер современной информационной войны. Взгляд китайских исследователей

В статье предоставлен анализ понимания и ведения информационной войны китайскими исследователями. Новые информационные вызовы, с которыми столкнулся Китай, показывают, насколько искусны китайские аналитики. Китайская республика влилась в мировое информационное противоборство и заняла в ней свою, специфическую нишу. Разработка рядов информационной безопасности как внутри Китая, так и в мировом пространстве воплотилась в информационную защиту, обеспечивающую Китаю безмятежное развитие.
Ключевые слова: информационная война, информационная безопасность, Китайская информационная политика, современные вызовы, информационное противоборство.

T.M. Yesnazarov, E.M. Uzhkenov
Information warfare in the views of the Chinese researchers

The article provides an analysis of understanding of information warfare by Chineseresearchers. New information challenges faced by China, show how adept the Chinese militaryanalysts.
Keywords: Information warfare, Chinese information security.

Е.М. Ужкенов, Т.М. Есназаров
Мао Цзэдун ішкі саясатының ұлтшылдық беталыстары

Мақалада қытайлық зерттеушілердің ақпараттық соғысты жүргізуі мен түсінуінің талдауы берілген. Қытайдың жаңа ақпараттық шабуылдары қытай сараптамасының қаншалықты жолға қойылғанын көрсетеді.
Түйін сөздер: Қытай, ақпараттық соғыс, ақпараттық шабуыл.

В последнее время в печати появляются все новые публикации о возникновении нового типа войн – «информационных войн», которые идут на смену традиционным. Выдающийся германский военный и политический деятель К. Клаузевиц сказал о том, что «война – есть продолжение политики другими средствами». В XXI веке можно сделать вывод о том, что информационная война есть основное средство современной мировой политики, доминирующий способ достижения духовной, экономической и политической власти. В современном мире, учитывая ценность информационных технологий, их роль в информационной войне, как наступательной, так и оборонительной очень важна.

В основе теоретических подходов китайских специалистов в области информационного противоборства – взгляды древнекитайского философа Сунь-Цзы. Он первым обобщил опыт информационного воздействия на противника. В своем трактате «Искусство войны» Сунь-Цзы писал: «Во всякой войне, как правило, наилучшая политика сводится к захвату государства целостным; разрушить его значительно легче. Взять в плен

армию противника лучше, чем ее уничтожить... Одержать сотню побед в сражениях – это не предел искусства. Покорить противника без сражения – вот венец искусства. Сунь-цзы объясняет важность владения информацией и приемами дезинформации противника для манипулирования его состоянием и действиями: «Если я покажу противнику какую-либо форму, а сам этой формы не буду иметь, я сохраню цельность, а противник разделится на части» [1, с.150].

Будущая война, возникновение которой, как считают китайские военные аналитики, может быть спровоцирована сбоем в компьютерных сетях промышленного сектора мировой экономики и будет представлять собой, по существу, бескомпромисную борьбу в информационной сфере. Такая война охватит всю совокупность военных, политических и экономических аспектов жизнедеятельности людей. На первом плане в ней окажутся информационные системы.

По мнению китайских исследователей, люди, участвующие в информационной войне отнюдь не солдаты (не носят военную форму, не стреляют). Однако они могут принимать стратегические решения в качестве персонала так называемых мозговых центров, основа которых специалисты высочайшей квалификации в области информационных технологий. Скорейшая мобилизация личного состава вооруженных сил в период развития конфликтов теряет свою актуальность. Вместо этого предусматривается «мобилизация» информационных центров и вступление их в войну первыми.

Воздействие на противника может осуществляться косвенным путем, например через Интернет. В этом случае противоборствующей стороне не всегда удастся определить, что это – несанкционированный доступ в информационную сеть компьютерного хакера или происки врага. Такой характер действий предусматривает наличие у каждого компьютерного солдата высокого уровня независимости и инициативы. Он в состоянии работать самостоятельно, без взаимодействия с кем-либо и, действуя в одиночку, вводить в информационные сети противника такое огромное количество бесполезных сведений, что из-за перегрузки каналов связи блокируется нормальная работа информационных систем последнего, снижается вероятность ответных действий. Таким образом, активно сочетая человеческий и искусственный интеллект, используя умелую организацию, можно ввергнуть противную сторону в состояние информационного хаоса.

Кроме того, как пишет Панарин, предполагается коренное изменение традиционных форм и способов вооруженной борьбы, утверждение приоритета концепции информационной войны и т. д. Информационные технологии – это ключ к овладению всеми остальным и технологиями стремительно развивающегося мира, и так как они поступательно социализируются, а сферы столкновения интересов людей все больше расширяются, то ведение информационного противоборства перестало быть занятием исключительно вооруженных сил.

В настоящее время новые концепции ведения операций быстро завоевывают себе право на жизнь. Информация уже сама по себе не только своеобразное оружие, но и ценный трофей. Качество, количество и скорость ее передачи представляют собой ключевые элементы информационного превосходства. По своему воздействию на объект она сопоставима с высокоточным оружием и средствами ведения электронной войны. Поэтому надежная защита информации, своевременное принятие контрмер по нейтрализации негативного воздействия являются основными пунктами подготовки и ведения информационной войны.

Итак, в информационный век средства и методы, концепции ведения войны коренным образом меняются. Противоборство воюющих сторон может мало повлиять на внешний материальный мир, вызвав разрушение информационных сетей. Шантаж и другие эффективные меры активного характера, применяемые посредством информационного воздействия, позволяют существенно ослабить противника или нанести ему поражение. Кровавый характер войны сменяется бескровной конфронтацией информационных систем. Игнорирование вопросов информационной войны в настоящее время недопустимо, иначе легко оказаться на задворках исторического процесса [2, с. 215-216].

В широком смысле информационная война – это крупномасштабные боевые действия с преобладанием информационной составляющей, характеризующиеся применением специально предназначенных для ее ведения воинских фор-

мирований и высокоточного оружия. Если основным средством достижения успеха на поле боя в XX веке были танки, то в будущем им станет компьютер. Это, в свою очередь, подразумевает применение компьютерных вирусов, способных разрушать программное обеспечение технических средств органов боевого управления и связи, инициировать сбои в системах управления и наведения высокоточного оружия и тем самым значительно снижать боевой потенциал противника. Война с широким использованием высокоточного оружия потребует существенного увеличения скорости добывания разведданных, времени предупреждения об ударах противника, улучшения взаимодействия командиров всех степеней, повышения маневренности войск, а значит, и эффективности всех видов информационного обеспечения. Самолеты, танки, корабли и ракеты, изготовленные с применением технологии «стелт», станут основной боевой техникой войск. Боевые действия с их участием, скорее всего, будут напоминать соревнование в быстроте обнаружения и уничтожения, и характеризоваться высокой интенсивностью и скоротечностью.

Китайские военные эксперты пристальное внимание уделяют зарубежным разработкам в области ведения информационной войны. Как и западные военные специалисты, они полагают, что информационная война не есть в прямом смысле война на поле боя, подготовкой к которой служат многочисленные учения и маневры войск. Вооруженные конфликты последнего времени побудили их выделить несколько характерных черт, присущих информационной войне.

Во-первых, «прозрачность» поля боя. Привычная «горячка боя» уступает место «хирургическим» методам работы подразделений информационной войны. Оператор компьютера может осуществлять непрерывный контроль за ситуацией, наблюдать отображаемое на дисплее расположение своих войск и войск противника, его объекты, концентрацию и перемещение его сил.

Во-вторых, общая координация действий войск посредством создания единого канала управления для всех боевых подразделений и подразделений тылового обеспечения. Все оперативные функции указанных формирований (разведка, управление, связь) в этом случае сводятся в единую систему. Например, оператор информационного центра, имея данные о количестве, составе и координатах выявленных целей противника, производит расчеты для распределения их по средствам поражения, определяет количество необходимых боеприпасов и т. д.

В-третьих, ведение боевых действий в реальном масштабе времени, т. е. немедленное реагирование на изменение боевой обстановки.

В-четвертых, точность ударов, отличающихся своеобразной чистотой и аккуратностью, подобной работе скальпеля хирурга.

Все это делает необходимым оснащение вооруженных сил передовыми информационными технологиями.

Такие вооруженные силы представляют собой новую категорию войск с самостоятельной теорией ведения боевых действий, особой организационно-штатной структурой, высоким уровнем подготовки личного состава и вооружением, полностью отвечающим требованиям информационной войны. Китайские военные эксперты скрупулезно перенимают опыт зарубежных коллег в данной области. Особенно пристальное внимание они уделяют исследованиям в США – единственной стране, где план создания армии нового типа уже имеется на бумаге и постепенно воплощается в жизнь.

Боевые формирования, предназначенные для ведения информационной войны, будут использовать технологии цифровой связи, целостную систему разведки и боевого управления, высокоточное оружие. Их арсенал пополнят радары нового поколения, системы опознавания типа «свой – чужой», элементы глобальных навигационных систем [3].

В целях приспособления к нуждам информационной войны организационно-штатная структура вооруженных сил претерпит изменения: численность сухопутных войск будет сокращаться, а ВМС и ВВС расти; возможно, появятся новые виды вооруженных сил, такие, как космические силы и информационно-компьютерные войска. Увеличится доля офицеров-профессионалов, особенно с инженерным образованием. Организация частей и подразделений будет основываться на оптимальной комбинации высоко обученного личного состава и высокотехнологичной техники; управление должно стать еще более гибким.

По взглядам руководства КНР, ее вооруженные силы в состоянии адекватно реагировать на изменения, происходящие в сфере мирового

военного строительства. Пока еще по разработкам и оснащению современным вооружением они отстают от развитых стран Запада. Однако китайские военные эксперты полагают, что в свете грядущих вооружённых конфликтов, в частности с применением информационных технологий, их армия способна соответствующим образом ответить противнику, ведь принцип максимального использования внутренних сил в противодействии внешним – в национальных традициях Китая. По уровню информационных технологий и информационного оружия Китай в будущей войне вряд ли сможет превзойти потенциального противника, поэтому его стратегическая линия будет направлена на активную оборону своих рубежей с максимальным привлечением внутренних ресурсов. В контексте информационной войны это означает усиление мер по маскировке своих войск, повышению активности противовоздушной обороны, атаке и перехвату боевых средств, применяющих высокоточное оружие, в момент, когда противник этого не ожидает, и т. д.

Китайские военные аналитики предполагают, что успешное ведение информационной войны потребует от вооруженных сил полного использования преимуществ территории страны и средств разведки в целях раннего выявления намерений противника, его подготовки к наступательным действиям; разработки, совершенствования и применения имеющихся на вооружении эффективных информационных технологий; усиления акцента на ведение мобильных боевых действий; организации операций по деморализации войск врага; формирования специальных сил ведения информационной войны, их оснащения современным оружием, разработанным на базе новых ИТ. Они уверены, что развитие информационных технологий неизбежно вызовет революцию в военном деле и эта революция уже началась. Те, кто первыми примут в ней участие, окажутся на гребне процесса развития человеческого общества, Указанная революция – это, прежде всего революция концепций, а потом уже прогресс в науке и технике, стратегии и тактике, обучении военному делу. Поэтому важнейшей проблемой, требующей тщательной проработки, является подготовка и ведение информационной войны [3].

Говоря об опыте Китайской Народной Республики на поле информационных битв, можно сказать, что страна очень преуспела. В Китае была создана мощная государственная система ведения информационного противоборства, которая позволяет осуществлять массированное применение сил и средств в нужное время. Ядром системы являются Исследовательское бюро при госсовете КНР и системно-аналитический центр министерства государственной безопасности. Китайская система ведения информационного противоборства наиболее эффективно действует в финансовой сфере. Она получает информацию от диаспор стран тихоокеанского региона и разведки. Осуществляется тотальный контроль над СМИ как внутри страны, так и в странах тихоокеанского региона. Значительное число газет, теле– и радиоканалов приобретены агентами и офицерами китайской разведки. Посредством контролируемых СМИ осуществляются активные комплексные информационно-психологические операции [4, с. 153-155].

Значительны успехи китайских спецслужб на территории США. Численность китайской диаспоры в Америке на конец 2010 года – около 3,794,673 млн. человек, что составляет 1,2% [5], основная ее часть сосредоточена на Тихоокеанском побережье, где китайская разведка имеет настолько сильные позиции, что американские спецслужбы не в состоянии полностью контролировать китайскую активность в таких городах, как Сиэтл, Лос-Анджелес, Сан-Франциско, Хьюстон.

Интересен факт, что США обвинили министерство обороны Китая в том, что китайская армия поддерживает направленную против США деятельность хакеров. Представитель министерства обороны Китая назвал эти обвинения в адрес китайских военных непрофессиональными и безосновательными [6].

Благодаря организованному мощному китайскому лобби КНР решает на территории США ряд стратегических задач: обеспечивает продвижение дешевых китайских товаров (Китай занимает третье место в списке стран-экспортеров для США), стимулирует рост китайской диаспоры за счет эмиграции из материкового Китая, добывает для китайской промышленности передовые технологии и научные разработки.

Я думаю, Китай, как одна из мировых империалистических стран, осознает всю важность понимания, проведения информационной вой-

ны, обеспечении информационной безопасности на локальной и мировой арене. За годы становления в одну из мировых держав Китайская республика набрала бесценный опыт ведения нового типы войны и вырвалась в лидеры информационного доминирования на глобальном уровне.

References

1 Sun'-Czy. Iskusstvovojny. PerevodNatal'jaRybal'chenko. – M.: Sofija, 2008. – 114 s.
2 Panarin I. InformacionnajavojnaiGeopolitika. – M.: Pokolenie, 2006. – 215 s.
3 Dezhin E. N. Informacionnajavojnapovzgljadamkitajskihvoennyhanalitikov //Voennajamysl'. 1999. №6.
4 Panarin I., Panarina L. Informacionnajavojnaimir. – M.: Olma-Press, 2003. – 153 s.
5 CentrperepisinaselenijaSShA. http://factfinder2. census. gov/faces/tableservices/jsf/pages/productview.xhtml?pid=DEC_10_SF1_QTP8&prodType=table
6 Vashingtonobespokoenaktivnost'jukitajskihhakerov. http://www. kp. ru/online/news/1386827/y

В статье предоставлен анализ понимания и ведения информационной войны китайскими исследователями. Новые информационные вызовы, с которыми столкнулся Китай, показывают, насколько искусны китайские аналитики. Китайская республика влилась в мировое информационное противоборство и заняла в ней свою, специфическую нишу. Разработка рядов информационной безопасности как внутри Китая, так и в мировом пространстве воплотилась в информационную защиту, обеспечивающую Китаю безмятежное развитие.