ПОДХОДЫ США И КНР К ИНФОРМАЦИОННОМУ ПРОТИВОБОРСТВУ

UNITED STATES OF AMERICA AND CHINESE PEOPLE'S REPUBLIC APPROACHES TO INFORMATION COUNTERING

УДК 355

ЧЕШУИН Сергей Анатольевич
кандидат технических наук, доцент
ПОЛОНЧУК Руслан Андреевич

CHESHUIN Sergey Anatolievich
Candidate of Technical Sciences, Associate Professor
POLONCHUK Ruslan Andreevich

Аннотация. *В статье обобщаются теоретические положения, раскрывающие сущность и содержание подходов к информационному противоборству, принятых в США и КНР. Авторы рассматривают взгляды американских и китайских военных специалистов на совершенствование*

информационного противоборства в целях обеспечения национальной безопасности государства.

Ключевые слова: *информационное противоборство; информационная война; информационно-коммуникационные технологии, кибербезопасность; национальная безопасность.*

Abstract.*The article summarizes the theoretical provisions that reveal the nature and content of the approaches to the information confrontation adopted in the United States and China. The authors consider the views of American and Chinese military experts on the improvement of information confrontation in order to ensure the national security of the state.*

Keywords: *informational confrontation; Information and communications technology (ICT), information war; cybersecurity; National security.*

В условиях постоянно изменяющейся военно-политической обстановки информация представляет для государства стратегический ресурс. В свою очередь, непрерывное совершенствование информационных технологий, их внедрение во все сферы жизнедеятельности вызвали появление ряда проблем. Основная из них – необходимость обеспечения информационной безопасности государства. Эксперты отмечают, что в данной сфере появились новые виды войн – информационные [5, С. 12].

По оценкам китайских военных специалистов, информационная война (или противоборство – термин встречающийся в китайской литературе) является совокупностью действий, направленных на уничтожение или временную нейтрализацию информационных систем противника, защиту собственных информационных систем, нацеленных на достижение превосходства над противником с помощью информации в качестве оружия [1, С. 65].

Как неоднократно отмечалось в аналитических документах Конгресса и

МО США Китайская Народная Республика (КНР) всесторонне и последовательно наращивает усилия в области информационного противоборства. Обладание собственной национальной военной стратегией, совершенствование сил, средств и способов ведения информационной борьбы формируют возможности военно-политического руководства Китая выигрывать локальные войны без борьбы с применением традиционных вооружений. Китайские специалисты отмечают, что информационная война (ИВ) Китая в современных условиях представляет, в первую очередь, метод ведения асимметричной войны против основного противника – США. В свою очередь, результаты анализа проводимых китайской стороны мероприятий в информационной сфере позволяют утверждать американским военным специалистам и политологам, что в КНР непрерывно происходит поиск оптимального подхода к адаптации всего положительного опыта информационного противоборства в интересах совершенствования вооруженных сил. Кроме того, сбор информации китайские специалисты осуществляют не столько путем шпионажа, но и через тщательное изучение теории и практики американских подходов ведения ИВ. Исследования американских военных теоретиков вооруженных конфликтов XXI века позволили выделить успешные действия в информационном пространстве. Например, такие аспекты ИВ как психологические операции, отрицание и дезинформация, по мнению китайских военных специалистов, обеспечивают благоприятные условия для одержания победы в конфликтах любой интенсивности.

Анализ военно-доктринальных документов США позволяет сделать вывод, что уже сейчас для американских военных специалистов, занимающихся планированием в области обороны, концентрация усилий Китая на ИВ представляет потенциальную угрозу национальной безопасности [4 , С. 23].

Информационная война – это борьба в интересах получения информации о противнике и предотвращения получения им информации о

состоянии и деятельности своих войск и сил. Она ведется для противодействия (нейтрализации) усилий противника по информационному воздействию и недопущению его противодействия, ввода в заблуждение противоборствующей стороны и недопущения дезинформации своих войск, а также с целью недопущения уничтожения своей информации противником.

По взглядам китайских военных специалистов, информационное доминирование является главным принципом информационной войны и определяется как возможность защиты собственных информационных систем и разрушение информационной структуры противника. По оценке китайских специалистов, информационное превосходство зависит не только от технологического превосходства, но и от новой тактики на поле боя. При этом понятие «поле боя» расширяется и уже не имеет четких границ. В операциях XXI века упор будет делаться на нанесение глубоких ударов по пунктам управления противника, центрам передачи информации и системам обеспечения. Особое внимание уделяется разрушению автоматизированных систем управления войсками противника, без которых применение высокоточного оружия будет неэффективным [2, С. 250].

Одной из разновидностей информационной войны является «кибервойна». Сам термин «киберпространство» определяется специалистами в области информационной войны как информационное пространство, моделируемое с помощью компьютерных технологий, в котором существуют объекты и символьное представление информации (место, в котором действуют компьютерные программы и циркулируют данные). Отмечается, что в основе «кибервойны» лежит выявление наиболее уязвимых звеньев в инфраструктуре государства, а также действия, направленное на уничтожение, блокирование информации в информационных, телекоммуникационных и электронно-вычислительных системах при помощи компьютерных атак («кибератак»).

По мнению китайских военных специалистов, существует ряд основополагающих принципов достижения победы в кибервойнах, наиболее

важными из которых являются:

- поражение или захват системы электроснабжения головного компьютера группировки противника;

- нанесение удара по системам дистанционной разведки, управления войсками и оружием, узлам связи, электронно-вычислительным центрам и другим ключевым сегментам информационной сети противника;

- создание искусственных условий по «перегрузке» компьютерной сети противника (DOS-атака) позволяет получить непосредственный контроль над потоками информации в системе управления войсками, материальными и энергетическими ресурсами (DOS (Denial Of Service) – отказ в обслуживании – *С.Ч., Р.П.*); заражение вирусами программных средств компьютерной сети противника – один из эффективнейших способов поражения компьютерной сети командных центров противника;

- использование достижений в области программных средств с целью несанкционированного, тайного проникновения в сеть управления противоборствующей стороны.

Учитывая современные риски кибербезопасности администрация США в сентябре 2018 года уточнила «Национальную стратегию кибербезопасности», где в частности отмечается что:

- Администрация обеспокоена растущими кибер-угрозами объектам собственности и вспомогательной инфраструктуры в космосе, поскольку эти объекты имеют критическое значение для таких функций, как позиционирование, навигация и синхронизация (positioning, navigation, and timing (PNT)); разведка, наблюдение и рекогносцировка (intelligence, surveillance and reconnaissance (ISR)); спутниковая связь (satellite communications); и мониторинг погоды (weather monitoring);

- Администрация будет настаивать на том, чтобы федеральные министерства и ведомства располагали необходимыми юридическими полномочиями и ресурсами для борьбы с транснациональной киберпреступной деятельностью, включая выявление и разбор бот-сетей,

теневых рынков и другой инфраструктуры, используемой для совершения киберпреступлений, и борьбы с экономическим шпионажем [6, С. 10];

- Правительственные структуры используют массивы данных для повышения защищенности на уровне сетевого оборудования через передачу производителям сведений об уязвимостях и угрозах. Вполне вероятно, что разработчики программного обеспечения будут производить несколько версий оборудования: для внутреннего пользования в США и на экспорт. Так, вычислительные сети государств, не являющихся союзниками и использующих американское сетевое оборудование, уже не могут противостоять отдельным классам компьютерных атак.

Для одержания победы в информационных войнах, по взглядам китайских военных аналитиков, необходимы следующие условия:

1) Цифровое поле боя – это сложная сетевая система, охватывающая все оперативное пространство. Она состоит из систем связи, управления и контроля, передачи разведывательных сведений, боевой компьютерной базы данных и терминалов пользователей, которые могут предоставить исчерпывающую оперативную информацию в реальном или близком к реальному масштабе времени. Назначение этой сетевой системы – применение информационной технологии для получения, обмена и использования цифровой информации в реальном масштабе времени, быстрый сбор информации по требованию командования, личного состава боевых и поддерживающих органов для ясного и четкого уяснения условий на поле боя и выработки и реализации оперативных планов. То есть обеспечивается широкая возможность использования географически распределенной силы.

2) Снабженные информацией войска («информатизированные» войска). В настоящее время многие развитые страны Запада рассматривают вопрос создания армий с высокой технологией информирования, а США уже активно реализуют планы формирования «информатизированных» войск [3, С. 25]. «Информатизированная» армия – это совершенно новая военная категория, с присущими ей теорией боевых действий, системой формирования, подбором

личного состава и вооружением, полностью соответствующими требованиям информационной войны. Предполагается, что силы, участвующие в ней, высоко интеллектуальны.

3) Наличие эффективных коммуникаций между объектами в боевом пространстве.

Китайские военные специалисты считают, что реализации концепции информационных войн существенно повлияет на характер ведения боевых действий и будет проявляться в следующем:

1) Информационные войны усилят соперничество в сфере информационного доминирования. Наличие и развитие боевой эффективности войск будет основываться, главным образом, на сборе, анализе, передаче и использовании информации;

2) Информационные войны расширят сферу вовлечения в военные действия, что проявится, главным образом, в двух областях (аспектах):

- усложнение в достижении победы в войнах. В информационный век необходимо будет не только устранить «материальную базу», обеспечивающую ведение противником войны, но и, кроме того, взять под контроль и уничтожить информационные системы противника, которые станут первостепенными целями при нанесении ударов;

- распространение границ войны на космическое пространство. Ключевые информационные системы передачи данных, местоопределения, наведения и связи будут размещаться в космосе;

3) Сокращение продолжительности боевых действий. С одной стороны, средства нападения будут высокоточными. С другой – в информационный век, по сравнению с индустриальным, цели, преследуемые воюющими сторонами, не будут связаны с полным окружением и уничтожением противника, а носить более ограниченный политический характер;

4) Придание боевым действиям цельного характера. В связи с тем, что информация будет передаваться быстро и не будет зависеть от рода войск или ограничена по времени, будущие войны станут беспрецедентно цельными.

Боевые действия на земле, море, в воздухе и космосе будут компактными, что будет характерно как для войн большого масштаба, так и для вооруженных конфликтов малой интенсивности. Граница между стратегическим, оперативным и тактическим звеньями станет нечеткой;

5) Изменение сути сосредоточения войск. Концентрация, главным образом, живой силы заменится на концентрацию преимущественно огневой мощи и информации, а количественная сторона сосредоточения войск и вооружения заменится на качественную.

При этом эксперты ведущих зарубежных стран отмечают, что в новых условиях оперативной обстановки при решении задач управления войсками и оружием существуют следующие проблемы:

- неполная, неточной информации о противнике и о своих войсках, а также необходимость немедленного принятия решения, для выполнения поставленной задачи в кратчайшие сроки и с минимальными потерями;

- значительные объемы получаемой и передаваемой информации на всех уровнях управления и достаточно низкая пропускная способность систем связи;

- краткость формы боевого распоряжения для его оперативного доведения до подчиненных сил и его содержание, которое должно точно отражать ясность боевых задач;

- определение приоритетности в выборе целей, средств, способов их поражения.

По оценкам китайских военных теоретиков, с учетом требований концепций и особенностей ведения информационных войн, произойдут изменения в составе и структуре вооружённых сил: количественная пропорция сухопутных войск будет сокращаться с одновременным возрастанием доли ВМС и ВВС; будут совершенствоваться боевое и техническое обеспечение и сокращаться материально-техническое; количество офицерского состава по сравнению рядовым и сержантским возрастет; увеличится число офицеров с технической подготовкой и уменьшится – с командной и штабной. Кроме того,

появятся новые воинские специальности [1, С. 89].

В силу специфики информационных войн и ограничений на военные расходы, военно-политическое руководство Китая в области технического оснащения Народно-освободительной армии Китая (НОАК) следует политике «больших исследований и новых технологий, меньшего производства и закупок вооружения». При этом его усилия сосредоточены на трех направлениях:

- завершение и пересмотр уже принятых проектов развития соединений и планов закупок;

- увеличение темпов исследований;

- совершенствование существующего вооружения.

Одновременно с увеличением доли производства нового оружия, военно-политическое руководство КНР неуклонно осуществляет практические мероприятия в области организации и ведения информационного противоборства по трем основным направлениям:

- подготовка квалифицированных кадров;

- совершенствование форм и способов информационных войн в ходе оперативной и боевой подготовки НОАК;

- непосредственное ведение информационных и психологических операций и противодействие им.

Для подготовки квалифицированных кадров в области информационного доминирования разработана специальная программа обучения, рассчитанная на три категории военнослужащих.

Первая категория – высшее звено управления НОАК. Как правило, это лица, чей возраст составляет более 40 лет. Основная задача их обучения – изучение основ информационных технологий и концепций ведения информационных войн.

Вторая категория – командиры соединений и частей ВС Китая. В основном, это лица, чей возраст составляет от 30 до 40 лет. Основная задача их обучения – изучение форм и методов ведения ИВ, а также изучение

основных принципов функционирования информационных систем.

Третья категория – кадровые офицеры, владеющие основами вычислительной техники и программирования, чей возраст, как правило, не превышает 30 лет. Главная задача их обучения состоит в углубленном изучении стратегии, форм и методов ведения ИВ с последующим их применением в кризисных ситуациях. В отличие от двух первых групп срок обучения этой группы гораздо продолжительнее.

Помимо этого, в программу обучения каждой из категорий, включены следующие вопросы:

- стратегия и тактика ИВ; методы и способы ведения ИВ; компьютерное моделирование ИВ; основы информационных технологий;

- принципы функционирования систем телекоммуникаций;

- обеспечение безопасности собственной информации и меры противодействия техническим средствам иностранных разведок [1, С. 113].

В настоящее время в Китае существует ряд центров подготовки специалистов в области информационного противоборства: Командная академия связи НОАК (Communications Command Academy) (Ухань, провинция Хубэй) является основным центром подготовки специалистов. В учреждении ведутся разработки новых методов и способов ведения информационных войн. Центры обучения также действуют при Университете информационных технологий (Information Engineering University) (Чжэнчжоу, провинция Хэнань), при Университете науки и техники (Scienceand Engineering University) и при Государственном оборонном научно-технологическом университете (National Defense Scienceand Technology University) в городе Эчен (провинция Хубэй). В Тяньцзиньском университете развернут интернет-центр военного образования, предназначенный для распространения знаний в военной области и информации о военном строительстве. Идет работа по созданию собственных компьютерных сетей для передачи данных в кратчайшие сроки.

В КНР также прилагают много усилий по привлечению высококлассных

специалистов, прошедших подготовку за рубежом, в том числе более ста тысяч китайцев, обучающихся и проживающих после окончания ВУЗов в США.

Непосредственно для проведения информационных операций привлекаются сотрудники спецслужб, выпускники различных специализированных высших учебных заведений вооруженных сил и Министерства государственной безопасности (МГБ), таких как Институт иностранных языков НОАК (г. Лоян, провинция Хэнань) и Институт кадрового менеджмента МГБ (Instituteof Cadre Management) в г. Сучжоу (провинция Цзянсу), а также гражданских ВУЗов.

Информационно-техническая подготовка в войсках рассматривается китайским военно-политическим руководством в качестве задачи стратегического значения, а соответствующая подготовка строится исходя из реальных условий современной войны. В настоящее время в вооруженных силах регулярно проходят тренировки и учения по вопросам информационной борьбы, одной из главных задач которых является отработка практических мероприятий по проведению и отражению «кибератак» в локальных и глобальных информационных сетях.

В условиях информационных войн роль специальных служб, осуществляющих сбор, обработку, анализ и доведение до руководства страны военно-политической, военно-технической и экономической информации, а также проведение информационных и психологических операций, значительно возрастает. В связи с этим, руководство КНР уделяет их развитию большое внимание.

В целях повышения возможностей национальных вооруженных сил по информационному противоборству, военно-политическим руководством Китая был осуществлен ряд практических мер.

В частности, в составе больших отрядов специального назначения НОАК, развернутых в каждом военном округе, созданы специальные подразделения компьютерного противодействия, имеющие на вооружении

современные средства внедрения в компьютерные сети противника на его территории и передачи снятой информации своему командованию по каналам тропосферной и спутниковой связи.

У отрядов есть возможность распространения вирусов в компьютерных сетях противника, способных нарушить работу его автоматизированных систем управления войсками, а также средства защиты собственных информационных сетей. Подразделения компьютерного противодействия могут использоваться и для ведения психологической войны.

Руководство НОАК считает, что подразделения и части должны обеспечиваться современной техникой для ведения информационно-пропагандистской деятельности. В этих целях создается современная АСУ управления войсками и оружием, система управления беспилотными летательными аппаратами и система связи с использованием компьютерных сетей.

Проведенный анализ литературы позволяет утверждать, что к перспективным видам информационно-психологического оружия НОАК стоит отнести:

- электронно-вирусное оружие;

- средства, позволяющие вклиниваться в трансляции радио- и телепрограмм;

- устройства создания радиопомех;

- одноразовые и многоразовые генераторы различных видов электромагнитной энергии, такие как взрывомагнитные, взрывные магнито-гидродинамические, пучково-плазменные.

Кроме того, в военно-научных кругах Китая все большее значение отводится отработке вопросов программно-электронного воздействия на информационные ресурсы противника, хранящиеся в компьютерных информационно-управляющих системах. Основным считается направление применения в ходе информационного противоборства электронно-вирусных средств, так называемого электронно-вирусного оружия (ЭВО).

Представляется возможным утверждать, что основными особенностями ЭВО считаются:

- дешевизна его производства при значительной эффективности воздействия;

- скрытность применения, автономность, длительность функционирования;

- возможность трансформации, многообразие способов внедрения;

- способность выводить из строя современные системы управления войсками и оружием.

К основным задачам, решаемым с применением ЭВО, стоит отнести:

- добывание информации (государственная или военная тайна противоборствующей стороны);

- введение противника в заблуждение, парализация систем управления, вмешательство в управление войсками и оружием противника.

В целях эффективной реализации потенциала электронно-вирусного оружия командованием НОАК в перспективе до 2025 года будут разработаны теория и принципы ведения электронно-вирусной войны, а также сформированы специальные части и подразделения.

Таким образом, постоянно совершенствуя концептуальную базу, техническую оснащенность, состав сил и средств, привлекаемых к информационным операциям, командование ВС США считает, что результативность таких операций зависит от решительности, быстроты и эффективной интеграции и синхронизации совместного информационного влияния на противника с привлечением политических, экономических и военных структур, необходимых для завоевания и удержания информационного превосходства над потенциальным противником. Информационные операции проводятся во всех фазах военной операции, взаимосвязаны с решением других ее задач, способствуют их выполнению, а также могут быть одной из главных ее составляющих.

Военно-политическое руководство Китая, рассматривая

последовательное внедрение странами Запада информационных технологий в военной области в качестве вызова национальной безопасности КНР, активизировало военно-теоретические изыскания по проблемам информационной войны, а также осуществляет практические шаги по созданию современной информационной инфраструктуры государства и повышению возможностей по ведению информационных операций.

Вопросы тактики и стратегии ведения информационных войн, разрабатываемые военными теоретиками НОАК, дают основание говорить об имеющейся в них своего рода «китайской специфике».

ЛИТЕРАТУРА (REFERENCES):

1. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018 / Office of the Secretary of Defense, 2018.
2. China's cyber activities // U.S.-China economic and security review commission. 2018.
3. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence // Journal of Strategic Security. 2018. Pp. 1-26.
4. Mandiant, APT1: Exposing One of China's Cyber Espionage Units // Alexandria. 2017.
5. Pickrell R. A dangerous game: responding to Chinese cyber activities // The Diplomat. 2017.
6. National cyber strategy of the United States of America// The White House. Office of the President. 2018.

Чешуин Сергей Анатольевич
кандидат технческих наук, доцент
заместитель начальника кафедры военного регионоведения
Военный университет Министерства обороны Российской Федерации
123001, г. Москва, Б. Садовая ул., д. 14.
sancesh@gmail.com

Полончук Руслан Андреевич
преподаватель кафедры военного регионоведения
Военный университет Министерства обороны Российской Федерации
123001, г. Москва, Б. Садовая ул., д. 14.
rus_mgs@gmail.com

Cheshuin Sergey Anatolyevich
Candidate of Technical Sciences, Associate Professor
Deputy Head of the Department of Military Regional Studies
Military University of the Ministry of Defence of the Russian Federation
B. Sadovaya ul., d.14, Moscow, Russia, 123001

Polonchuk Ruslan Andreeevich
Lecturer at the Department of Military Regional Studies
Military University of the Ministry of Defence of the Russian Federation
B. Sadovaya ul., d.14, Moscow, Russia, 123001

23.00.00 – Политология