УДК 355.02

РОЛЬ ИНФОРМАЦИОННОГО ОРУЖИЯ В ВОЕННО-ПОЛИТИЧЕСКОЙ СТРАТЕГИИ США

© 2012 г. **Г.Б. Корсаков**[*]
Институт мировой экономики и международных отношений РАН, Москва

В статье рассматривается развитие информационного оружия, а также различные аспекты его применения, связанные с началом использования цифровых технологий в военной сфере. Раскрывается роль информационного оружия как фактора скрытого давления США на противника путём целенаправленного воздействия на его информационную инфраструктуру и информационное пространство для получения стратегических преимуществ и закрепления за собой в XXI веке статуса информационной сверхдержавы.

Ключевые слова: *информационное оружие, стратегия информационного сдерживания, информационные и телекоммуникационные технологии, информационное пространство, киберугрозы, информационная безопасность, информационная война.*

XXI век характеризуется взрывным ростом объёма циркулирующей в мире информации наряду со стремительным увеличением мощности технических средств по её обработке и передаче. В то же время ускоряющаяся динамика развития информационных и телекоммуникационных технологий, предоставление широких возможностей для повышения эффективности всей информационной инфраструктуры постиндустриального общества, создают и множество проблем в различных областях мировой политики, прежде всего в области международной и национальной безопасности.

В результате широкого применения новейших информационных технологий претерпели изменения как средства вооружённой борьбы, так и стратегия и тактика ведения современных войн, появились концепции, учитывающие факторы информационной уязвимости сторон. Возрастает зависимость процессов, происходящих в различных областях военной деятельности, качества функционирования информационно-коммуникационных сетей и циркулирующей в них информации. В то же время появляется широкий спектр методов и средств воздействия на подобные сети, например путём вывода из строя их отдельных структурных элементов или манипуляции информацией.

Между тем, благодаря стремительному распространению информационных и телекоммуникационных технологий происходит концентрация мощи (политической, экономической, военной) в нескольких мировых центрах влияния,

[*] **КОРСАКОВ Георгий Борисович – кандидат политических наук, старший научный сотрудник ИМЭМО РАН.** E-mail: Koroleva@imemo.ru

которые при определённых условиях могут оказаться потенциальными оппонентами Соединенных Штатов. Поэтому США форсируют разработку стратегии информационного сдерживания возникающих центров силы, опираясь на своё абсолютное превосходство в области спутниковой коммуникации и в Интернете. Поддержание лидерства в области развития информационных и телекоммуникационных технологий рассматривается американским военно-политическим руководством в качестве важнейшего компонента глобального информационного превосходства, которое, в свою очередь, составляет критически важный элемент политики обеспечения национальной безопасности.

Концептуальные основы информационного противоборства

Доктринальная проработка вопросов ведения информационного противоборства в США началась сразу же по завершении первой войны в Персидском заливе (1991 г.), в которой американскими вооружёнными силами были впервые применены новейшие информационные технологии. Так, в директиве Министерства обороны (МО) *TS 3600.1* от 21 декабря 1992 г., были сформулированы основные положения стратегии информационного противоборства [26].

Дальнейшая теоретическая разработка этих вопросов была оформлена в виде официального издания так называемых единых доктрин. В феврале 1996 г. Комитет начальников штабов (КНШ) ввёл в действие «Доктрину борьбы с системами управления»[14]. В ней излагались принципы борьбы с этими системами для информационного противоборства в военной сфере. В декабре 1998 г. в силу вступила «Объединённая доктрина информационных операций», согласно которой информационная операция – это комплекс мероприятий по манипулированию информацией для достижения и удержания всеобъемлющего превосходства над противником через воздействие на информационные процессы, происходящие в системах управления [28]. Например, во время кризисов информационные операции могут помочь удержать противника от проведения акций, наносящих ущерб США и их союзникам.

В документах были определены цели, задачи и основные принципы информационного противоборства, обязанности руководящих органов и должностных лиц по их организации и планированию в мирное время и в условиях кризисной обстановки. Кроме того, в них были перечислены требования к разведывательному обеспечению информационных операций, а также к подготовке личного состава, обеспечивающего их планирование и проведение. Как следовало из документов, эффективное информационное противоборство должно обеспечить возможность навязать противнику ложное видение оперативной обстановки, принудить его к ведению военных действий в невыгодных для него условиях. Это достигается в основном благодаря проведению комплекса мероприятий, позволяющих, с одной стороны, нарушить процесс принятия решений противником, а с другой – обрабатывать информацию в своей системе управления эффективнее и быстрее, чем это может сделать противник.

Пришедшие к власти в начале XXI века республиканцы значительно повысили внимание к проблеме противоборства в информационном пространстве [18].

В феврале 2003 г. президент Дж. Буш-мл. одобрил «Национальную стратегию безопасности киберпространства», которая, по сути, была первой доктри-

нальной инициативой, определившей необходимость координации и сосредоточения усилий всех федеральных ведомств на защиту национального информационного пространства [39]. В развитие этого доктринального документа в октябре 2003 г. Министерством обороны была опубликована «Дорожная карта информационных операций» [25]. С реализации поставленной в этом документе задачи начались постепенная отработка и введение основных положений стратегии информационного противоборства в состав военной доктрины, а также формирование структуры для управления операциями в информационном пространстве.

В свою очередь КНШ утвердил в феврале 2006 г. документ «Информационные операции». Как следовало из документа, информационные операции представляют собой комплекс мероприятий по воздействию на людские и материальные ресурсы противника для того, чтобы затруднить или сделать невозможным принятие верного решения с одновременной защитой своих информационно-коммуникационных сетей и компьютерных систем. Такие операции включали в себя пять основных составляющих: радиоэлектронную борьбу, психологические операции, операции в информационно-коммуникационных сетях, военную дезинформацию, оперативную безопасность. Были определены и вспомогательные элементы информационных операций, необходимые для достижения успеха операции в мирное и в военное время, в том числе: физическое воздействие, связь с общественностью, поддержка структурами Минобороны публичной дипломатии и др. [24].

Директива Министерства обороны *D 3600.1*, введённая в действие 14 августа 2006 г., впервые чётко определила основные задачи и функции информационных операций, в целом означающие комплексное применение средств радиоэлектронной борьбы, операций в информационно-коммуникационных сетях, психологических операций, военной дезинформации и оперативной безопасности [22]. В документе отмечалось, что информационные операции проводятся «в целях информационного воздействия, введения в заблуждение, нарушения работы компьютерных систем, искажения информации, дезорганизации баз данных и лишения противника возможности их использования, извлечения информации из компьютерных систем и баз данных противника при одновременном обеспечении защиты своей информации и информационной инфраструктуры».

Документ вводил в действие принцип разделения информационных операций на три категории: атака на компьютерные сети, защита компьютерных сетей, обеспечение доступа к компьютерным сетям противника и их использование в своих интересах.

Аналогичные директивы были изданы всеми видами ВС США [23].

Пришедшая к власти в начале 2009 г. администрация демократов продолжила активно развивать стратегию информационного противоборства и защиты национальной информационной инфраструктуры. Сразу же после вступления в должность президент Б. Обама отдал распоряжение о проведении тщательного анализа мероприятий федеральных ведомств по организации комплексной эффективной защиты национальных информационно-коммуникационных сетей, а также о разработке стратегии борьбы в информационном пространстве. Как следовало из официального заявления Б. Обамы, «кибершпионаж и преступления в информационно-коммуникационных сетях стали

нарастающей тенденцией. Поэтому кибербезопасность – высший приоритет национальной безопасности страны в XXI веке» [42].

Эта речь совпала по времени с выходом в свет «Обзора политики в киберпространстве», представленного президенту специальной комиссией, проводившей анализ состояния дел в области защиты информационного пространства.

В обзоре содержались рекомендации по совершенствованию безопасности национальной информационной инфраструктуры [15]. В частности, утверждалось, что федеральные ведомства слишком забюрократизированы и разобщены в своих действиях в области кибербезопасности. Особо подчёркивалось, что требуется незамедлительно выработать приемлемые правовые нормы в области кибербезопасности для национальной юрисдикции, суверенной ответственности государств и порядка силового реагирования на киберугрозы.

Из доклада также следовало, что подходы США к обеспечению кибербезопасности не соответствуют темпам возрастания угрозы. Отмечалось, что национальная безопасность практически полностью зависит от функционирования информационно-коммуникационных сетей, которые обеспечивают жизнедеятельность всей национальной инфраструктуры, в первую очередь федеральных ведомств, отвечающих за оборону и безопасность. В соответствии с рекомендациями американских специалистов, предлагалось создать пост координатора по кибербезопасности, подотчётного непосредственно президенту.

Эти предложения практически полностью совпали с рекомендациями экспертов из вашингтонского Центра стратегических и международных исследований, сделанными ими в декабре 2008 г. в докладе «Обеспечение безопасности киберпространства для 44-го президента США» [51].

В марте 2010 г. стало известно об основных направлениях реализации программы повышения эффективности противодействия кибератакам на американские информационно-коммуникационные сети и базы данных. Работы ведутся в соответствии с «Инициативой всеобъемлющей национальной кибербезопасности» (*The Comprehensive National Cyber Security Initiative*) под руководством Совета национальной безопасности США [35]. К её выполнению привлечены все федеральные ведомства, а также структуры правительств штатов, ответственные за обеспечение безопасности информационного пространства. Следует отметить, что в неё вошли документы, разработанные ещё при предшествующей республиканской администрации. Это изданные в январе 2008 г. Президентская директива по обеспечению национальной безопасности № 54 и Президентская директива по обеспечению внутренней безопасности № 23.

«Инициатива» предусматривает дальнейшее совершенствование мониторинга работы федеральных информационно-коммуникационных сетей, а также введение в действие программы «Надёжное интернет-соединение», нацеленной на уменьшение количества точек подключения компьютерных систем федеральных ведомств и учреждений к внешним информационно-коммуникационным сетям с тем, чтобы своевременно обнаруживать случаи вторжения. Предполагаемые расходы на реализацию «Инициативы» могут составить от 40 млрд. до 100 млрд. долл. Всего в ней предусматривается 12 основных направлений работ, связанных со всесторонней защитой национального информационного пространства и фиксированием всех попыток несанкционированного проникновения.

Американские специалисты намерены прежде всего чётко определить допустимые границы в борьбе с киберугрозами, а также создать условия для полной информированности военно-политического руководства США об уязвимости компьютерных систем, обеспечивающих жизнедеятельность национальной информационной инфраструктуры, а также для закрытия технологических брешей в компьютерных системах, и своевременно предпринять необходимые меры для парирования возможных кибератак.

Другая важнейшая задача, обозначенная в «Инициативе», – защита баз данных от всего спектра вероятных киберугроз. Её предлагается решать путём расширения технических и оперативных возможностей федеральных ведомств, ответственных за национальную безопасность. Кроме того, планируется обеспечить более тщательный контроль каналов поставок новейших информационных технологий федеральным структурам, отвечающим за национальную оборону и безопасность. Предполагается, что это полностью исключит возможность приобретения ими технических средств, способных нанести ущерб национальной безопасности.

Ещё одно масштабное направление реализуемой «Инициативы» – комплекс мероприятий по качественному улучшению системы подготовки специалистов в области информационной безопасности. Предлагается также повысить эффективность координации финансируемых из федерального бюджета НИОКР в этой сфере и внедрить действенные механизмы их своевременной переориентации, чтобы исключить неоправданные расходы на дублирующие исследования.

Планируется разработка стратегических подходов для эффективного противодействия всем видам киберугроз. Для этого предлагается провести комплекс мероприятий, начиная с модернизации государственных структур, отвечающих за информационную безопасность, и заканчивая определением места и роли федерального правительства в этом процессе, с тем чтобы обеспечить непрерывный контроль за функционированием национальных информационно-коммуникационных сетей и управление ими как единым комплексом. Это, по мнению американских специалистов, только первый шаг на пути к обеспечению надёжной кибербезопасности. Все действующие центры быстрого реагирования на киберугрозы должны быть объединены в единую структуру, что позволит контролировать ситуацию в компьютерных системах в режиме реального времени и существенно повысить качество анализа предпринимаемых противником кибератак. Предлагается провести мероприятия, направленные на создание структур киберконтрразведки, их оснащение новейшими техническими средствами с внедрением самых современных технологий, предназначенных для повышения информационной безопасности закрытых каналов связи и передачи данных.

В мае 2011 г. президент Б. Обама утвердил «Международную стратегию для киберпространства», которая декларирует комплексный подход американского военно-политического руководства к политике в глобальном информационном пространстве [27]. Документ подтверждает, что информация и национальная информационная инфраструктура в целом – это стратегический ресурс. Подчеркивается, что в XXI веке государство имеет весьма ограниченные возможности управления и контроля в киберпространстве. Между тем, в формирующейся полицентричной системе международных отношений всё более

активную роль начинают играть различные негосударственные структуры (в том числе враждебно настроенные к США), которые нередко обладают сопоставимыми по мощности информационными ресурсами.

Особый акцент специалисты делают на международном сотрудничестве в области обеспечения информационной безопасности, подчёркивая стратегический подход американского руководства к вопросам кибербезопасности. При этом главная роль в обеспечении информационной безопасности всей национальной инфраструктуры отводится Минобороны.

Среди основных политических приоритетов развития национальной информационной инфраструктуры, наряду с развитием национальной экономики, защитой информационно-коммуникационных сетей, ужесточением законодательства в информационной сфере, развитием международного сотрудничества, созданием эффективной структуры для управления Интернетом и обеспечения фундаментальных принципов свободы в Интернете, американские специалисты важное место отводят военному компоненту.

Впервые в официальных документах особое внимание уделено информационному сдерживанию потенциальных противников США. При этом структуры коллективной безопасности (такие как НАТО) позволят, по мнению американских специалистов, эффективно применять стратегию информационного сдерживания по отношению к государствам – оппонентам и негосударственным структурам. Важное место в документе отведено также проблеме выработки необходимых норм международного права в области информационной безопасности.

В развитие этого доктринального документа МО издало «Стратегию по операциям в киберпространстве», которую в июле 2011 г. представил, выступая в Университете национальной обороны, заместитель министра обороны У. Линн. При этом он заявил: «США оставляют за собой право в соответствии с законами войны ответить на кибератаки пропорциональным и справедливым образом в то время и в том месте, которое мы выберем» [16].

В «Стратегии» указывается, что киберпространство будет рассматриваться как сфера оперативной деятельности (в дополнение к четырём основным). Всего в документе названы пять стратегических инициатив, выполнение которых позволит Минобороны защитить национальную инфраструктуру: 1. Признание киберпространства приоритетной сферой оперативной деятельности; 2. Применение «активной защиты» информационно-коммуникационных сетей и компьютерных систем; 3. Эффективное взаимодействие Минобороны с другими федеральными ведомствами и частными компаниями в области обеспечения информационной безопасности; 4. Налаживание активного сотрудничества с союзниками и партнёрами США в области коллективной защиты от киберугроз; 5. Увеличение финансовых и материальных ресурсов, вкладываемых в развитие научно-технической базы кибербезопасности, а также в подготовку профильных высококвалифицированных специалистов.

В целом, из доктринальных документов, формулирующих основные составляющие стратегии информационного противоборства, следует, что Вашингтон декларирует необходимость обладать надёжным и отвечающим современным требованиям национальной обороны и безопасности потенциалом ведения информационного противоборства. При этом подчёркивается возрастающая роль информационного оружия, как важнейшего элемента в планах ведения войн нового поколения, отмечается, что рост зависимости эффектив-

ности боевых действий от новейших цифровых технологий неизбежно ведёт к росту уязвимости всей национальной информационной инфраструктуры.

Принципиальный вывод всех документов заключается в необходимости надёжной и всеобъемлющей защиты национального информационного пространства и всей информационной инфраструктуры в целом.

Формы и методы применения информационного оружия

Под информационным оружием американские специалисты понимают совокупность специально организованного и структурированного информационного трафика, который, наряду с новейшими информационными и телекоммуникационными технологиями, позволяет целенаправленно видоизменять (уничтожать, искажать, блокировать, копировать) информацию, преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование носителей информации, дезорганизовывать работу технических средств, компьютерных систем и информационно-коммуникационных сетей [44; 45; 47; 48].

Другими словами, под информационным оружием понимается арсенал средств несанкционированного доступа к информации и выведения из строя электронных систем управления противника. При этом средства информационно-психологического воздействия в состоянии не только причинить вред здоровью, но и привести к блокированию на неосознаваемом уровне свободы волеизъявления человека, утрате способности к политической, культурной и другой самоидентификации, манипуляции общественным сознанием и даже разрушению единого информационного и духовного пространства.

Появление информационного оружия, по мнению американских специалистов, принципиально меняет механизм эскалации вооружённых конфликтов, так как даже выборочное применение информационного оружия по объектам военной и гражданской информационной инфраструктуры противника может завершить конфликт на его ранней стадии. Обладание информационным оружием обеспечивает политическое и военно-стратегическое преимущество над государствами, у которых его нет.

Причём, как и ядерное, информационное оружие может служить не только для политического давления, но и для сдерживания. По оценке некоторых американских экспертов, эффект целевого информационного воздействия на противника сравним с применением ОМУ, и угроза подвергнуться такому воздействию может стать важным фактором сдерживания потенциального агрессора. Эффективность такой угрозы напрямую зависит от уровня технологического развития и масштаба использования компьютерной техники в информационных системах государства. Например, компьютерная система может быть либо уничтожена физически, либо из неё может быть похищена критически важная информация, либо её программное обеспечение может быть изменено в результате вирусного проникновения или хакерской атаки.

Один из ведущих американских специалистов в области информационного противоборства, профессор Университета национальной обороны М. Либики считает, что в будущем информация станет основным средством сдерживания вооружённых конфликтов [30]. По его мнению, единая разведывательно-информационная инфраструктура, состоящая из сети космических, воздуш-

ных, наземных и морских датчиков различного назначения, позволит контролировать любую военную активность на планете и, следовательно, применять превентивные меры. В таких условиях, по мнению М. Либики, любые действия потенциального противника будут абсолютно прозрачны для противоположной стороны и международного сообщества в целом. Соответственно, противник может быть лишён даже самой возможности провести военные приготовления, поскольку глобализация мировых информационно-коммуникационных сетей позволит парализовать и блокировать его системы управления, тем самым нанеся значительный ущерб военному потенциалу. В своих работах Либики выделил семь основных форм информационного противоборства: борьба с системами управления, информационно-разведывательная, электронная, психологическая, хакерская, кибернетическая и экономическая [31].

Борьба с системами управления противника предусматривает их физическое уничтожение и отсечение командных структур противника. Такая борьба может достигаться непосредственным уничтожением управляющих структур и разрушением коммуникаций, связывающих системы управления с подчиненными подразделениями. Ценность информационных операций против систем управления состоит в том, что они могут оказаться особенно эффективными на ранних стадиях развития конфликта и служить основой для достижения быстрой победы над противником.

Информационно-разведывательные операции предполагают оперативный сбор, обработку и доведение до конечного пользователя максимально полной информации о противнике в режиме реального или близком к реальному времени. Создание многоуровневой системы сбора данных позволяет получать максимально полную картину ситуации в районе боевых действий и облегчает распределение информации между пользователями.

Электронная борьба представляет собой снижение информационных возможностей противника. В соответствии с этим она подразделяется на радиоэлектронную (в частности, путём постановки активных и пассивных помех), которая считается главным направлением, криптографическую (искажение и ликвидация собственно информации) и борьбу с коммуникационными системами противника.

Психологические операции представляют собой комплекс мероприятий по распространению специально подготовленной информации для воздействия на эмоциональное состояние, мотивацию, аргументацию действий, принимаемые решения и поведение оппонентов в благоприятном для США и их союзников направлении. По своим масштабам они могут быть стратегическими, оперативными и тактическими и включают в себя четыре основных компонента: подрыв гражданского духа, деморализацию личного состава ВС, дезориентацию высшего политического и военного руководства и войну культур. Основным инструментарием ведения таких операций являются национальные и транснациональные СМИ, а также глобальные информационно-коммуникационные сети.

Хакерская борьба представляет собой действия с применением программных средств (программно-математическое воздействие на информационно-коммуникационные сети), направленные на использование, искажение, подмену или уничтожение информации, содержащейся в базах данных компьютеров и информационно-коммуникационных сетей, а также на снижение эффективности функционирования либо вывод из строя самих компьютеров и компью-

терных систем. Конкретные приёмы хакерской борьбы носят самый разнообразный характер.

Кибернетическая борьба охватывает полный комплекс проблем и аспектов (организационные, доктринальные, стратегические, тактические, технические) ведения информационных операций и в настоящее время становится всё более актуальной именно в военной сфере. При этом понятие кибернетической борьбы относится скорее к организационной форме информационного противоборства, чем собственно к борьбе с информационной инфраструктурой противника. Более того, кибернетическая борьба подразумевает использование информационной инфраструктуры противника в своих целях.

Экономическая борьба. Развитие технических возможностей средств связи, передачи и накопления информации привело к тому, что экономика государства и его финансовая сфера также стали представлять собой важную цель для информационного воздействия.

Ещё одна форма применения информационного оружия (хотя и опосредованная) – так называемая «культурная экспансия». Задействованные в ней американские специалисты считают, что модернизация, проводимая сегодня в ряде стран мира, требует не просто экономических преобразований и инновационных технологий. Она якобы невозможна без изменений во внутрицивилизационном укладе, направленных на привнесение в него «западных демократических ценностей». Об этом подробно пишут в своей книге «Значение культуры: как культурные ценности формируют человеческий прогресс» известные американские эксперты Л. Харрисон и С. Хантингтон [19].

Как следует из многочисленных американских исследований в области информационного противоборства, технология проведения кибератак на информационно-коммуникационные сети и компьютерные системы достаточно изучена и состоит, главным образом, из следующих приёмов и методов [6; 20]:

• Атака на крупные информационно-коммуникационные узлы для нанесения значительного ущерба объектам национальной инфраструктуры противника;

• Поиск «чёрного хода» в защите определённой компьютерной системы противника путём кибератаки на секретный ключ криптографической защиты, который используется для усиления стандартной криптозащиты баз данных;

• Возможность использования для взлома компьютерной системы противника «человеческого фактора» в период проведения технических и регламентных работ, когда секретные файлы остаются открытыми;

• Создание инструментов распределённого нападения, приводящих к отказу в работе компьютерных систем противника, использование «троянских» вирусов (маскирующихся под безобидные программы), а также совершенствование традиционных средств радиоэлектронной борьбы;

• Вбрасывание в компьютерные системы противника управляемых вирусов, которые могут парализовать работу компьютеров;

• Атака на компьютерные системы противника с применением вирусов-«червей», запускающих бесконечный цикл распространения, в результате чего информационный трафик значительно возрастает, начинаются перегрузки и сбои в работе компьютеров;

• Применение специальных методик «моментального замедления Интернета»;

• Установка «жучков» в розетках для подключения информационно-коммуникационных устройств в конференц-залах, компьютерных классах, телефонных и кабельных шкафах;

• «Копание в мусоре» – наиболее популярный метод добывания списков паролей и другой секретной информации.

Технологическим инструментарием применения информационного оружия служит «Глобальная информационная сеть» (*Global Information Grid*), которая создается в интересах Минобороны и связанных с ним разведывательных структур для обеспечения доступа к единым информационным ресурсам всех военных баз, командных структур, боевых платформ и пунктов временной дислокации [32]. Планируется, что прежние информационно-коммуникационные сети МО, например «Глобальная система оперативного управления», будут постепенно встраиваться в «Глобальную информационную сеть». Работы проводятся под руководством Агентства информационных систем Минобороны.

Основным техническим средством ведения радиоэлектронной борьбы служит глобальная система радиоэлектронной разведки «Эшелон», позволяющая перехватывать информацию, передаваемую по электронным каналам связи и прослушивать телефонные переговоры в любой точке планеты. Эта система обладает широкими возможностями контроля любого радиоэфира и кабельных сетей*.

Для координации всех профильных структур Минобороны, отвечающих за информационное противоборство, в июне 2009 г. в составе Объединённого стратегического командования США было сформировано Киберкомандование (*U.S. Cyber Command*), достигшее в мае 2010 г. состояния начальной оперативной готовности. Возглавил новое командование генерал-лейтенант Кит Александер, сохранивший также свой пост руководителя Агентства национальной безопасности [3]. Общая численность персонала АНБ (штаб-квартира в Форт-Мид, штат Мэриленд) составляет около 120 тыс. человек, из них три четверти работают в региональных центрах, расположенных по всему миру. В интересах АНБ действуют около 4 тыс. станций радиоперехвата, развёрнутых на всех континентах. Бюджет АНБ равен около 15 млрд. долл. Для сравнения: по состоянию на январь 2011 г. численность сотрудников ФБР составляла около 35 тыс. человек, а на финансирование их деятельности в 2010 г. из федерального бюджета было израсходовано 7,9 млрд. долларов.

Таким образом, действия американского военно-политического руководства в области информационного противоборства направлены на создание единого центра управления всеми операциями в информационном пространстве с сосредоточением в нём необходимых технических средств и оперативных возможностей.

---

* Созданная и развернутая Соединёнными Штатами во взаимодействии с Великобританией, Канадой, Австралией и Новой Зеландией система «Эшелон» вместе со спутниковой системой перехвата радиоволн и трафика беспроводных коммуникаций способна фиксировать телефонные переговоры, факсы, электронную почту и даже данные, передаваемые по спутниковым терминалам. Во взаимодействии с системой «Эшелон» работают технические средства союзников и партнёров США, которые следят за радиоэфиром в своих географических пространствах. Система «Эшелон» состоит из следующих основных элементов: 1. Орбитальная группировка спутников слежения, которые контролируют огромное количество электронных средств связи; 2. Суперкомпьютеры, способные анализировать до 10 млрд. сообщений в сутки; 3. Пункты прослушивания, развернутые по всему миру (на американских военных базах, на территориях, закамуфлированных под гражданские организации) и осуществляющие перехват, запись и декодирование сообщений [20].

Концепция «информационной войны»

В начале 1990-х годов США вплотную приступили к изучению и проработке проблем, связанных с противоборством в информационном пространстве, – так называемой *информационной войной*. В США под этим термином понимается комплексное информационное воздействие на систему государственного и военного управления противника, которое уже в мирное время приводило бы к принятию благоприятных для США решений, а в ходе конфликта полностью парализовало бы функционирование структуры управления противника. Одновременно с наступательным воздействием информационная война предполагает обеспечение надёжной защиты национальной информационной инфраструктуры.

Реализация положений концепции «информационной войны» означает перенос акцента противоборства с традиционных форм воздействия (огонь, удар, манёвр) в информационно-интеллектуальную область – в процесс принятия решений. Основная цель такой войны – дезинтеграция и расчленение целостности управления группировкой противника на изолированные друг от друга, дезориентированные и неуправляемые элементы и их последующий вывод из строя.

По мнению американских аналитиков, информационная война состоит из действий, предпринимаемых для получения информационного превосходства, под которым понимается достижение военно-стратегического преимущества за счёт более высокого, чем у противника, информационного потенциала, который позволяет держать противника в постоянном напряжении, одновременно повышая боевую устойчивость собственных сил. Основные задачи информационной войны при этом заключаются в выведении из строя компьютерных систем противника; проникновении в компьютерную базу данных стратегически важных ведомств и получении доступа к секретным документам путём взлома информационно-коммуникационных сетей противника; получении доступа к новейшим (в том числе и засекреченным) разработкам в области высоких технологий; получении стратегических данных о внешней и военной политике государств; проведении экономической разведки; отслеживании в режиме реального времени неавторизованными пользователями фактов прохождения оперативной секретной информации; в организации тотальной слежки за гражданами разных государств; отключении связи со спасательными службами и системами оповещения; ведении пропагандистской войны в информационном пространстве; организации информационной безопасности путём противодействия любым попыткам противника внедриться в компьютерные системы, обеспечивающие национальную безопасность; в борьбе с кибертерроризмом [30; 33; 45].

Практическая реализация концепции «информационной войны» осуществляется путём проведения *информационных операций*, которые представляют собой комплекс взаимосвязанных по цели, месту и времени мероприятий и акций, направленных на управление процессами манипулирования информацией для достижения и удержания информационного превосходства над противником путём воздействия на его информационную инфраструктуру при одновременной защите собственной. Соответственно, все информационные операции подразделяются на наступательные и оборонительные.

Наступательные и оборонительные информационные операции могут проводиться по единому замыслу и плану и взаимно дополнять друг друга. Они ориентированы на одни и те же объекты воздействия, в качестве которых могут выступать органы управления государства – оппонента и его вооружённых сил; информационные системы гражданской инфраструктуры (телекоммуникационные, транспортные, энергетического комплекса, финансового и промышленного секторов); управляющие элементы военной инфраструктуры (системы контроля, связи, разведки, боевого управления, тылового обеспечения, управления оружием); общество в целом (гражданское население и личный состав вооружённых сил); руководящий состав и персонал автоматизированных систем государственного и военного управления, участвующий в стратегических решениях.

Информационная война представляет собой не просто вид обеспечения операций вооружённых сил путём нарушения процессов контроля и управления войсками противника, радиоэлектронного подавления, морально-психологического воздействия и т.п., но выходит далеко за пределы перечисленных проблем. Об этом говорят результаты исследований, проведённых специалистами корпорации РЭНД ещё в конце 1990-х годов [4].

В этих и других исследованиях впервые появился термин «стратегическая информационная война» [47]. Такая война, по мнению авторов, представляет собой «использование государствами глобального информационного пространства и инфраструктуры для стратегических информационных операций и уменьшения воздействия на собственный информационный ресурс». Следует отметить, что появление подобной терминологии существенным образом отличается от официальной трактовки информационной войны, закреплённой в доктринальных документах Минобороны и введённой в оборот в начале 1990-х годов, которая рассматривала такую войну в достаточно узком смысле.

По мнению экспертов корпорации РЭНД, изменения в общественно-политической жизни ряда государств, вызванные быстрыми темпами информатизации и компьютеризации общества, ведут к пересмотру геополитических взглядов военно-политического руководства, к возникновению новых стратегических интересов (в том числе и в информационном пространстве), а следовательно, и к изменению политики, проводимой этими странами. Авторы подчёркивают, что глобальные противоречия требуют новых средств и методов разрешения, а именно воздействия на стратегический информационный ресурс. При этом они выделили ключевые особенности информационной войны: сравнительно низкую стоимость создания средств информационного противоборства; возможность беспрепятственно «нарушать» традиционные государственные границы при подготовке и проведении информационных операций; возможность манипулировать информацией; изменение приоритетов в деятельности стратегической разведки, которые смещаются в область завоевания и удержания информационного превосходства; сложность обнаружения начала информационной операции; сложность создания коалиции против агрессора, развязавшего информационную войну; наличие потенциальной угрозы территории США.

Ключевым понятием, введённым в исследованиях, является классификация стратегической информационной войны первого и второго поколений. При этом война первого поколения рассматривалась наряду с традиционными средствами противоборства. Подчёркивалось, что она больше ориентирована

на дезорганизацию деятельности систем управления противника и проводится скорее как обеспечение действий традиционных сил и средств. Отмечалось, что такое восприятие информационной войны свойственно начальному этапу осмысления проблемы. Так, стратегическая информационная война первого поколения определялась как «один из нескольких компонентов будущего стратегического противоборства, применяемый совместно с иными инструментами достижения цели». Другими словами, понятие «стратегическая информационная война первого поколения» фактически вобрало в себя основные методы информационной войны.

Стратегическая информационная война второго поколения определяется американскими специалистами как «принципиально новый тип стратегического противоборства, вызванный к жизни информационной революцией, вводящей в область стратегического противоборства информационное пространство и другие сферы (прежде всего, экономику и финансовый сектор) и продолжающийся долгое время». Отмечалось, что развитие и совершенствование подходов к ведению войны второго поколения в перспективе может привести к полному отказу от традиционного применения военной силы, поскольку скоординированные информационные операции могут позволить обойтись без этой крайней меры. Подчёркивалось также, что если последствия войны первого поколения ещё можно прогнозировать с использованием существующих методик, то второе поколение информационной войны весьма трудно прогнозировать, и существующие методики прогноза могут быть применены к анализу последствий весьма условно.

При определённой трансформации взглядов на проблему ведения информационной войны, по мнению американских специалистов, изменяются и задачи, которые нужно решать для достижения поставленной цели.

Для информационной войны первого поколения – это огневое подавление элементов информационной инфраструктуры государственного и военного управления противника; ведение радиоэлектронной борьбы; получение разведывательной информации путём перехвата и расшифровки информационных потоков, передаваемых по каналам связи; осуществление несанкционированного доступа к информационным ресурсам противника с последующим их искажением или хищением; формирование и массовое распространение по информационным каналам противника или глобальным информационно-коммуникационным сетям дезинформации для воздействия на оценки, намерения лиц, принимающих стратегические решения; получение интересующей информации путём перехвата открытых источников информации.

Для войны второго поколения – это создание атмосферы бездуховности и безнравственности, негативного отношения к культурному наследию; манипулирование общественным сознанием социальных групп населения для формирования политической напряжённости и хаоса; дестабилизация отношений между политическими движениями в целях провокации конфликтов, обострения политической борьбы; снижение уровня информационного обеспечения органов государственного и военного управления, затруднение принятия ими стратегических решений; дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов государственного управления; провоцирование социальных, политических, национальных и религиозных столкновений; инициирование забастовок, массовых беспорядков и

других акций социально-экономического протеста; подрыв международного авторитета государства-оппонента, его сотрудничества с другими странами; нанесение ущерба жизненно важным интересам государства-оппонента в различных сферах.

Примечательно, что в июне 2010 г. тогдашний министр обороны Р. Гейтс утвердил документ о замене в американских вооружённых силах термина «психологические операции» термином «военные операции по информационному обеспечению». Таким образом продолжаются активные усилия по дальнейшему повышению эффективности специальных информационных операций для достижения информационного превосходства над противником. Особое значение при этом американское руководство отводит операциям по «обезглавливанию», основными целями которых являются автоматизированные центры государственного и военного управления, системы контроля и связи, политические и военные лидеры, главари международных террористических организаций, «полевые командиры».

По мнению профессора М. Либики, такие операции могут стать решающим фактором для исхода всей военной кампании, особенно если они проведены в нужное время и нужном месте. При этом удары, нанесённые по структурам стратегического управления, могут оказаться даже более эффективными, чем устранение какого-либо «неуправляемого» политического или военного лидера противника [30]. Операции по «обезглавливанию» могут проводиться и в отношении государств, политический курс которых не соответствует стратегическим установкам Вашингтона. При проведении таких операций возможно как физическое устранение политического лидера, так и его моральная и политическая дискредитация в глазах местного населения и мирового сообщества[*]. Для подобных операций применяются подразделения специального назначения американских вооружённых сил[**]. При этом, по мнению М. Либики, не обязательно использовать огневые средства поражения. Наибольший эффект могут дать различные средства информационного воздействия – компьютерные вирусы, электромагнитные импульсы и отключение электроэнергии, так как для их эффективного применения даже не нужно знать точные координаты пунктов стратегического управления противника.

Отметим, что теоретическая проработка различных аспектов ведения информационной войны ведётся в США уже долгое время. Ещё в 2001 г. в корпорации РЭНД вышло в свет исследование «Операции против лидеров противника» [21]. Его автор, С. Хосмер, рассматривая различные формы применения таких операций, выделил из них три основных: 1. Операции, направленные непосредственно против политического лидера; 2. Операции, предназначенные для инициирования и содействия в смещении политического лидера посредством внутренних заговоров или восстаний; 3. Операции, содействую-

[*] Образцом операции по дискредитации политического лидера государства-оппонента в глазах местного населения и мирового сообщества стали мероприятия против бывшего президента Югославии С. Милошевича.

[**] Примером одной из таких операций служит устранение 2 мая 2011 г. на территории Пакистана лидера международной террористической сети «Аль-Каида» У. бен Ладена. «Террорист номер один в мире» был ликвидирован (по официальной версии. – *Г.К.*) одним из подразделений «морских котиков» – структурным компонентом сил специальных операций ВС США.

щие смещению политического лидера в результате вмешательства военной силы извне. В целом, по мнению С. Хосмера, физическое устранение в результате такой операции политического лидера может привести к деградации всей системы стратегического управления противника, а успешно проведенная операция по его ликвидации может к тому же негативно отразиться на морально-психологическом состоянии войск противника.

Об этом пишут и другие американские специалисты [33; 45].

В любом случае, по их мнению, метод «материального поощрения» за действия, отвечающие стратегическим интересам Соединённых Штатов, применяемый американским командованием по отношению к политическим и военным лидерам противника, намного выгоднее, чем трата значительных материально-технических ресурсов, а также другие политические и экономические издержки, сопутствующие проведению полномасштабной военной операции (главная из которых – риск для жизни американских военнослужащих).

Важную роль в информационной войне американское руководство отводит Интернету, который также становится мощным стратегическим ресурсом. В январе 2010 г. госсекретарь США Хилари Клинтон провозгласила новую американскую стратегию, главной целью которой является «борьба с диктаторскими режимами через Интернет» [13]. При этом выбор критериев отбора целей для реализации этой стратегии остаётся за американским военно-политическим руководством.

Главнейший элемент таких информационных операций – так называемое «международное общественное информирование», осуществляемое Государственным департаментом, а непосредственный инструментарий – различные сегменты Интернета, в том числе, социальные сети. Как показывает пример интернет-ресурса «Викиликс», потенциал социальных сетей настолько высок, что может вызвать кризис политической власти одновременно на территориях нескольких государств. При этом региональные масштабы народных волнений способны перерасти в глобальные.

Наряду с наступательным аспектом ведения информационной войны американское военно-политическое руководство уделяет серьёзное внимание и защите национального информационного пространства и информационной инфраструктуры в целом. Заместитель министра обороны У. Линн, координирующий все вопросы информационной безопасности, выступая в июне 2009 г. в вашингтонском Центре стратегических и международных исследований, заявил, что «компьютерные системы и базы данных Минобороны постоянно подвергаются кибератакам со стороны иностранных спецслужб, а также различных структур и хакеров, заинтересованных в получении закрытой информации военного назначения» [36]. Например, в 2007 г. в результате спланированной хакерской атаки вышли из строя сразу 1,5 тыс. компьютеров Минобороны (по оценке тогдашнего министра обороны Р. Гейтса, ведомство каждый день выдерживает несколько сотен кибератак только из стран, которые считаются союзниками или партнёрами Соединённых Штатов).

Между тем, своими главными оппонентами в глобальном информационном пространстве американское военно-политическое руководство считает прежде всего Китай и Россию. Об этом оно неоднократно заявляло в отчётах, посвящённых проблеме утечки национальных секретов и участии в этом спецслужб разных стран [52]. По признанию У. Линна, случаи взломов компьютерных

систем Минобороны учащаются и становятся всё более изощрёнными. В своей статье «Защита нового пространства: киберстратегия Пентагона» он пишет, что «в последние десять лет ежедневно происходит несколько тысяч случаев внедрения и зондирования американских военных и гражданских компьютерных систем, а случаи считывания информации исчисляются миллионами... В результате противники США получили тысячи секретных документов, включая чертежи новейших систем вооружений, планы боевых операций, а также данные оперативного наблюдения» [34]. Как следует из статьи, самой массированной хакерской атаке на свои компьютерные системы Минобороны подверглось в 2008 г. Тогда одна из закрытых информационно-коммуникацинных сетей министерства была атакована хакерами, в результате было похищено множество военных секретов, непосредственно относящихся к сфере национальной безопасности. Последовавшие вслед за этим усилия военного руководства по противодействию кибератакам стали поворотным пунктом в американской стратегии кибербезопасности: начала создаваться мощная и многослойная защита информационно-коммуникационных сетей.

Серьёзную озабоченность по этой проблеме высказывает и непосредственный подчиненный Линна, генерал-лейтенант К. Александер. В докладе, сделанном в сенатском комитете по делам вооружённых сил, он отметил, что хакеры ежедневно совершают несколько сотен тысяч попыток взлома и вирусного инфицирования компьютерных систем МО [3]. Главным оппонентом США в глобальном информационном пространстве К. Александер считает прежде всего Китай. По его мнению, увеличение масштабов кибератак на информационную инфраструктуру Пентагона и предприятий американского оборонно-промышленного комплекса в будущем чревато серьёзными осложнениями. Китай, по мнению Александера, может расширить свои возможности в данной сфере и попытаться получить определённый контроль над отдельными сегментами Интернета, что, вероятно, будет идти вразрез с интересами США в области национальной безопасности.

Об этом пишет в исследовании «Управление Интернетом в эпоху киберуязвимости» и Р. Нейк из влиятельного нью-йоркского Совета по международным отношениям [29]. США, по его мнению, в значительной мере зависят от реализации мероприятий по борьбе с киберугрозами. Однако в связи с ростом масштабов этих угроз и постоянной трансформации их характера соответствующие структуры Пентагона и других федеральных ведомств просто не успевают своевременно разрабатывать необходимые меры противодействия. В ходе реализации инициативы Минобороны по защите информационного пространства должно быть обеспечено решение первостепенных задач, пишет Нейк. Он предлагает объединить в единое целое ресурсы всех федеральных структур США, занимающихся защитой информационно-коммуникационных сетей. К этой задаче, по его мнению, обязаны присоединиться и частные фирмы, выполняющие заказы по контрактам с Пентагоном. Необходимо также более чётко сформулировать задачи, которые придётся решать Киберкомандованию, и определить систему приоритетов его деятельности. Кроме того, по мнению Нейка, необходимо выявить уязвимые места национальной информационной инфраструктуры и разработать стандарты информационной безопасности. Наконец, в Минобороны следует сформировать группу специального реагирования, которая будет располагать всеми средствами для противодейст-

вия кибератакам и пресечения всех попыток взлома компьютерных систем на самых ранних этапах.

С этими выводами согласуется и позиция другого высокопоставленного сотрудника Минобороны, старшего аналитика Ш. Браймли. В статье «Обеспечение безопасности в общих пространствах» он обращает внимание на существующую уязвимость закрытых информационно-коммуникационных сетей министерства [9]. Он считает, что информационное пространство остаётся единственной областью боевых действий, где у США имеются равные противники. В этом отношении наибольшую опасность для США, по его мнению, представляет Китай, власти которого к середине XXI века намерены добиться такого уровня развития информационных и телекоммуникационных технологий, который позволит им обеспечить полную победу в информационной войне. Именно поэтому Вашингтон считает постоянный рост импорта китайских микросхем в США большой проблемой для национальной безопасности[*].

О важности всеобъемлющей защиты информационного пространства говорят и другие американские эксперты. Так, генерал в отставке У. Кларк (занимал пост верховного главнокомандующего Объединёнными вооружёнными силами НАТО в Европе, командовал вооружёнными силами альянса во время войны в Югославии в 1999 г.) и П. Левин (специалист в области информационной безопасности) в статье «Обеспечение безопасности информационной магистрали: как повысить уровень электронной защиты Соединённых Штатов» прямо указывают, что одна из главнейших проблем, стоящих перед американским руководством, – обеспечить аутентичность и надёжность профильной высокотехнологичной продукции и комплектующих, поставляемых из-за рубежа, в первую очередь из Китая [12].

Как следует из статьи, существуют способы негласного обнаружения специально сконструированных дефектов в поставляемых микросхемах. У. Кларк и П. Левин акцентируют особое внимание на том, что в XXI веке противник может избрать в качестве мишени не только информационно-коммуникационные сети и программное обеспечение, но и микрочипы, являющиеся элементом любого компьютера, т.е. всё то, что составляет основу национальной информационной инфраструктуры. Об этом же пишут и другие американские авторы[38; 43], обращая внимание на то, что активной проработкой проблемы обеспечения информационной безопасности Минобороны начало заниматься уже в начале 1990-х годов, т.е. с начала использования цифровых технологий в военной сфере [32]. Таким образом, как следует из предпринимаемых с начала 1990-х годов усилий по всестороннему развитию концепции «информационной войны», американское военно-политическое руководство стремится закрепить за США в XXI веке статус информационной сверхдержавы.

[*] Когда речь идёт об информационной безопасности, в первую очередь рассматривается защита информационно-коммуникационных сетей и программного обеспечения (*software*). Между тем, сами компьютерные системы (*hardware*) не менее уязвимы. Так, например, процесс производства микрочипа, насчитывающий порядка 400 операций, позволяет с легкостью внести в микросхемы умышленные дефекты, либо повредить их. Поэтому компьютер с повреждённой микросхемой представляет собой «мину замедленного действия», поскольку выведение его из строя происходит задолго до кибератаки – ещё на стадии конструирования, либо производства, а выведенные из строя микросхемы не могут быть исправлены и окончательно превращаются в «спящие элементы».

* * *

Престиж любой страны оценивается её успехами в развитии и использовании цифровых технологий в такой же мере, как и прогрессом в области развития ракетно-космической техники и атомной энергетики. В мире создан широчайший спектр информационных средств (от микропроцессоров размером в миллиметр до суперкомпьютеров с объёмом памяти в тысячи гигабайт и вычислительной способностью порядка 10^{15} операций в секунду), стремительно растёт и количество самих компьютеров.

Принципиально изменились задачи, решаемые с их помощью. Преимущественно вычислительные функции первых компьютеров уверенно дополняются широким спектром возможностей, предоставляемых информационными и телекоммуникационными технологиями.

В результате, цифровые технологии, объединяясь с другими средствами обработки, передачи, хранения и использования информации, образуют новую общественную среду – информационную. А информация постепенно становится таким же стратегическим ресурсом общества и государства, как и традиционные (материальные, энергетические, людские) ресурсы.

Ещё до недавнего времени американское руководство прогнозировало потенциал государств-оппонентов в пространстве, включавшем три основных измерения – политическое, экономическое и военное. Сегодня к ним добавилась новая сфера – информационная. И хотя она ещё до конца не сформирована, уже очевидно, что в дальнейшем возникнет потребность существенного пересмотра основных понятий в традиционных областях. В формирующемся информационном обществе ключом к успеху, по мнению американского руководства, будет умелое управление информационными возможностями и ресурсами, т.е. стратегическое планирование.

Так, аналитики корпорации РЭНД Дж. Аркуилла и Д. Ронфелд ещё в 1999 г. в докладе «Рождение неополитики: формирование американской информационной стратегии» сделали выводы о том, что традиционная стратегия претерпевает существенные и глубокие изменения [5]. По мнению аналитиков, информация и коммуникации всегда были важны для стратегии, а их роль постоянно возрастала вследствие появления многих причин. Во-первых, это технологические инновации: стремительный рост обширной новой информационной инфраструктуры, включающей не только Интернет, но и кабельные сети, спутники для прямого вещания, сотовые телефоны и т.п. Во-вторых, быстрое распространение нового типа коммуникаций: множество государственных и негосударственных структур непосредственно обмениваются важной информацией. В-третьих, понятия «информация» и «мощь» всё более переплетаются и становятся неразрывно связанными между собой.

Информационная стратегия пока ещё не определена однозначно, и американские аналитики в основном придерживаются двух точек зрения. Одна (технологическая) рассматривает в качестве приоритетной проблему информационной безопасности и защиты информации в компьютерных системах. Авторы этой группы исследований прежде всего ищут пути защиты от хакерских атак государств-оппонентов и террористических организаций [20; 43; 58]. Другое направление составляют работы, связанные с политическим и идеологическим контекстом происходящих процессов информатизации, в которых информационная стратегия рассматривается как способ выражения «мягкой силы» аме-

риканских стратегических установок для распространения своего влияния на руководство и население стран-оппонентов [46; 54; 59]. Сторонники такого подхода считают, что информационная мощь позволяет Соединённым Штатам «мягко» руководить ситуацией в мировой политике, отказываясь зачастую от «жёстких» методов реализации глобального доминирования, которое опирается в основном на традиционные средства (прежде всего на военную силу).

Однако аналитики обоих направлений ставят общую цель – выработать единый взгляд на то, чем должна стать американская информационная стратегия в XXI веке и как её интегрировать в общую стратегию национальной безопасности. При этом главную стратегическую цель информационного сдерживания они видят в воздействии не на системы вооружений, а на личность человека, принимающего стратегические решения на начальных этапах возникновения конфликта. От такого воздействия, по их мнению, и зависит эффективность стратегии информационного сдерживания.

В соответствии с программой стратегических оценок Национального разведывательного совета США в 2008 г. были проведены исследования, в которых изучалось и оценивалось мнение ведущих американских экспертов по проблеме трансформации современного общества под воздействием, в том числе, и информационной революции. Результаты были обобщены в докладе «Глобальные тенденции – 2025: меняющийся мир» [17]. В нём отмечалось, что информационные технологии превратились в один из наиболее важных факторов, способствующих динамичной трансформации современного общества, его переходу от индустриального общества к информационному. Среди основных тенденций мирового развития, ставящих перед США потенциальные проблемы, американские специалисты отмечали следующие:

- стремительное развитие информационных технологий и различия в восприятии результатов информационной революции в разных регионах мира могут привести к обострению межгосударственных отношений;
- в результате информационной революции могут возникнуть новые негосударственные структуры, которые существенно трансформируют глобальную экономику, что, в свою очередь, затронет места проживания людей и вызовет новую масштабную волну миграции населения планеты;
- информационная революция существенно скажется на механизмах управления обществом и создаст новых политических игроков;
- геополитические тенденции, которым содействует информационная революция, могут обозначить новые вызовы Соединённым Штатам.

Таким образом, потенциал информационного оружия уже осознан американским экспертным сообществом*. Растёт понимание необходимости придать информационному оружию наивысший приоритет в военно-политической стратегии США.

---

* В американских научных публикациях в последнее время в отношении информационного оружия даже появился термин «оружие массовых разрушений» (*weapon of mass disruption*) в противовес традиционному термину «оружие массового уничтожения» (*weapon of mass destruction*) [50].

Список литературы

1. *Корсаков Г.Б.* Тенденции развития военной политики Вашингтона // США ❖ Канада. 2011. № 2. С. 22–40.

2. *Роговский Е.А., Шариков П.А.* Пентагон усиливает кибероборону // США ❖ Канада. 2011. № 1. С. 51–60.

3. *Alexander Keith.* Lt Gen. Testimony (Confirmed as the First Commander U.S. Cyber Command) to the Senate Committee on Armed Services. 15.04.2010.

4. *Arquilla J., Ronfeldt D.* In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica: RAND, 1997.

5. *Arquilla J., Ronfeldt D.* The Emergence of Neopolitik: Toward an American Information Strategy. Report MR-1033-OSD. Santa Monica: RAND, 1999.

6. The Battle for Hearts and Minds: Using Soft Power to Undermine Terrorist Networks / Ed. by A. Lennon. Cambridge: Cambridge University Press, 2004.

7. *Borchgrave De A., Cilluffo F., Cardash S., Ledgerwood M.* Cyber Threats and Information Security: Meeting the 21st Century Challenges. Washington: CSIS, 2001.

8. *Bremmer I.* Democracy in Cyberspace: What Information Technology Can and Cannot Do // Foreign Affairs. November/December, 2010. P. 86-92.

9. *Brimley S.* Promoting Security in Common Domains // The Washington Quarterly. July 2010. P. 119-132.

10. *Butler R.* Deputy Assistant Secretary of Defense for Cyber and Space Policy. Testimony before the House of Representatives Committee on Armed Services Subcommittee on Strategy Forces. 21.04.2010.

11. *Castells M.* Communication Power. Oxford: Oxford University Press, 2009.

12. *Clark W., Levin P.* Securing the Information Highway: How to Enhance the United States Electronic Defenses // Foreign Affairs. November/December. 2009. P. 5-17.

13. *Clinton Hillary.* Remarks on Internet Freedom. Speech. Washington. 21.01.2010.

14. Command and Control Warfare. Joint Publication 3–13.1. Washington. Joint Chiefs of Staff. February 1996.

15. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. Washington. The White House. May 2009.

16. Department of Defense Strategy for Operating in Cyberspace. Washington. U.S. Department of Defense. July 2011.

17. Global Trends-2025: A Transformed World. National Intelligence Council. Washington. November 2008.

18. *Graham B.* Bush Orders Guidelines for Cyber Warfare // The Washington Post. 7.02.2003.

19. *Harrison L., Huntington S.* Culture Matters: How Values Shape Human Progress. New York. 2000.

20. *Hildreth S.* Cyber Warfare: Background and Issues for Congress. Congressional Research Service Report for Congress. RL 30735. 19.06.2001.

21. *Hosmer S.* Operations against Enemy Leaders. Santa Monica: RAND, 2001.

22. Information Operations. Directive D 3600.1. Washington. DoD. 14.08.2006.

23. Information Operations. Directive 10–7. Washington. U.S. Department of Air Force. 6.09.2006.

24. Information Operations. Joint Publication 3–13. Washington. Joint Chiefs of Staff. 13.02.2006.

25. Information Operations Roadmap. Washington. DoD. 30.10.2003.

26. Information Warfare. Directive TS 3600.1. Washington. DoD. 21.12.1992.

27. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington. The White House. May 2011.

28. Joint Doctrine for Information Operations. Joint Publication 3–13. Washington. Joint Chiefs of Staff. December 1998.

29. *Knake R.* Internet Governance in an Age of Cyber Insecurity. New York. Council on Foreign Relations. 2010.

30. *Libicki M.* Cyberdeterrence and Cyberwar. Santa Monica: RAND, 2009.

31. *Libicki M.* What is Information Warfare? Santa Monica: RAND, 1995.

32. *Libicki M.* Who Runs What in the Global Information Grid: Ways to Share Local and Global Responsibility. Santa Monica: RAND, 2000.

33. *Lonsdale D.* The Nature of War in the Information Age: Clausewitzian Future. London. 2004.

34. *Lynn W.* Defending a New Domain: The Pentagon's Cyberstrategy // Foreign Affairs. September/October 2010. P. 97-108.

35. *Lynn W.* Deputy Secretary of Defense. Remarks. National Space Symposium. Colorado Springs. 14.04.2010.

36. *Lynn W.* Protecting the Domain: Cybersecurity as a Defense Priority. Speech. Washington. CSIS. 15.06.2009.

37. *Malander R., Riddile A., Wilson P.* Strategic Information Warfare: A New Face of War. Santa Monica. RAND, 1996.

38. *McGiffert C.* Chinese Soft Power and Its Implications for the United States: Competition and Cooperation in the Developing World. Washington: CSIS, 2009.

39. The National Strategy to Secure Cyber Space. Washington. The White House. February 2003.

40. *Nye J.* Soft Power: The Means to Success in World Politics. New York: Public Affairs, 2004.

41. *Nye J.* The Future of American Power: Dominance and Decline in Perspective // Foreign Affairs. November/December 2010. P. 2-12.

42. *Obama Barack.* National Framework for Strategic Communication. Washington. The White House. 2009.

43. *O'Neil M.* Cyberchiefs: Autonomy and Authority in Online Tribes. London. 2009.

44. *Pincus W.* Pentagon Reviewing Strategic Information Operations // The Washington Post. 27.12.2009.

45. *Post D.* In Search of Jefferson's Moose: Notes on the State of Cyberspace. Oxford: Oxford University Press, 2009.

46. Public Sentinel: News Media and Governance Reform / Ed. by P. Norris. Washington: The MIT Press, 2009.

47. *Rattray G.* Strategic Warfare in Cyberspace. London: The MIT Press, 2001.

48. *Rid T., Hecker M.* War 2.0: Irregular Warfare in the Information Age. Westport, 2007.

49. *Sartori A.* Deterrence by Diplomacy. Princeton: Princeton University Press, 2005.

50. *Schmidt E., Cohen J.* The Digital Disruption: Connectivity and the Diffusion of Power // Foreign Affairs. November/December 2010. P. 75-85.

51. Securing Cyberspace for the 44th Presidency. Washington. CSIS Commission on Cybersecurity for the 44th Presidency. December 2008.

52. Securing Our Nation's Cyber Infrastructure. Washington. The White House. Office of the Press Secretary. 29.05.2009.

53. *Shirky C.* The Political Power of Social Media: Technology, the Public Sphere, and Political Change // Foreign Affairs. January/February 2011. P. 28-41.

54. Soft Power and U.S. Foreign Policy: Theoretical, Historical and Contemporary Perspectives / Ed. by Parmar I., Cox M. New York, London, 2010.

55. Soft Power Superpowers: Cultural and National Assets of Japan and the United States / Ed. by Watanabe Y., McConnell D. New York. 2008.

56. Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities / Ed. by W. Owens, K. Dam, H. Lin. Washington. 2010.

57. *Wiener N.* Cybernetics: or Control and Communication in the Animal and Machine. Cambridge: The MIT Press, 1948.

58. *Wilson C.* Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. Congressional Research Service Report for Congress. RL32114. 17.10.2003.

59. *Wolf Ch., Rosen B.* Public Diplomacy: How to Think About and Improve it. Santa Monica: RAND, 2004.