Е.А. РОГОВСКИЙ

ГЛОБАЛЬНЫЕ АМБИЦИИ США В ЦИФРОВУЮ ЭПОХУ

Роговский Евгений Александрович, *к.э.н., руководитель Центра проблем военно-промышленной политики Института США и Канады РАН*
123995, Москва, Хлебный пер., 2/3.
E-mail: rogowsky@mail.ru

Аннотация

Статья посвящена исследованию политических проблем доминирования Соединенных Штатов в глобальном киберпространстве. Рассматриваются исторические вопросы формирования киберкомандования США и военных стратегий использования кибероружия. Особое внимание уделяется политологическому анализу фактов уязвимости американских информационных систем.

Ключевые слова: *информационное превосходство, доминирование в киберпространстве, киберстратегии Пентагона, программа «свобода интернету», уязвимость информационных систем.*

В настоящее время и международный вес государства, и конкурентоспособность бизнеса во многом определяются тем информационным потенциалом, которым они располагают. А информационные ресурсы правительств разных стран, равно как и разных фирм, существенно различаются.

Когда цель взаимодействия состоит в извлечении какой-либо выгоды (политической или экономической), различия в уровнях информационно-технологических потенциалов определяют преимущества одних пользователей относительно других и создают ситуации информационного преобладания (превосходства). При этом есть основания полагать, что с учётом качественной составляющей такого рода «цифровой разрыв» со временем не сокращается, а, напротив, нарастает.

Методы использования такого разрыва в интересах одной стороны и в ущерб другой быстро совершенствуются – соответственно, возрастают и угрозы информационной безопасности, которым подвергаются пользователи киберпространства. Информационное превосходство становится одним из решающих факторов политического (и военного) противостояния, а также конкурентной борьбы.

«Америка не заинтересована в честной борьбе с кем бы то ни было. Мы хотим превосходить во всех системах» – заявил командующий армией США в Европе генерал Ходжес [1]. Нам представляется, генерал Ходжес изложил суть не только военной политики США в Европе, но и всей американской внешней политики. Доминирование во всех глобальных сферах – на земле, на море, в воздухе, в информационном пространстве – вот цель американской политики.

Доминирование Соединенных Штатов в киберпространстве означает, что США должны сохранять в нем свободу действий, одновременно не давая такой свободы противнику. Такого рода идея информационного доминирования, зафиксирована в ряде концептуальных документов Пентагона (Joint Vision 2020, Cyberspace Operations Concept Capability Plan 2016–2028 [2] и других).

Речь идёт о свободе проникновения в информационное поле других стран и одновременно о противодействии свободному проникновению в информационное поле США зарубежных пользователей. Иначе говоря, о последовательной политике смещения в свою пользу определённого баланса между анонимностью и транспарентностью пользователей киберпространства, между уровнем суверенности стран и уровнем транспарентности их национального информационного пространства (включающего персональные данные элит и иные чувствительные сведения).

В настоящее время отвечающие такой политике технологические возможности, – хотя они с очевидностью нарушают положенные в основу устава ООН принципы, сложившиеся во второй половине XX века, – стали доступными для бизнеса и широко используются в глобальной конкурентной борьбе. Соответственно, миру навязываются американские принципы и стандарты международной информационной безопасности (МИБ). Главное – обеспечить доминирование лидера, сделать мир транспарентным для себя: в этом и состоят, по нашему мнению, глобальные амбиции США в цифровую эпоху.

В целом можно сказать, что формирование политики Соединённых Штатов в киберпространстве ещё отнюдь не завершено, и прежде всего по причине очень быстрого развития информационно-коммуникационных технологий. Различным аспектам этой американской политики была посвящена вышедшая в 2014 г. в издательстве «Международные отношения» моя книга «Кибер-Вашингтон: глобальные амбиции». Однако в цифровую эпоху время бежит очень быстро, а потому материал этой книги уже нуждается в дополнениях и комментариях, которые и составили основное содержание настоящей статьи.

НЕМНОГО ИСТОРИИ

В начале XX века знаменитый американский историк и стратег адмирал Альфред Мэхэн (Alfred T. Mahan) отмечал, что Мировой океан является «Великим общим достоянием» (пространством) (Great Common), которым никто не обладает, но все пользуются. Он сформулировал известный закон «**геополитики морской силы**»: «Чтобы доминировать в мире, необходимо иметь неограниченную возможность пользоваться и ставить под свой контроль все, что относится к Великому общему достоянию».

В 1970–1980 гг. полковник Джон Бойд (John Boyd) предложил концепцию так называемого OOOD-цикла принятия решения (первоначально применительно к боевым действиям на стратегическом уровне): наблюдение, формулировка задачи, принятие решения, действие (англ. observe-orient-decide-act – OOOD Loop). Её основной тезис заключается в том, что побеждает тот, кто быстрее проходит этот цикл, иными словами, доминирует во времени.

Информационное доминирование – это вопрос комплексный (многоаспектный). Здесь важно иметь преимущество и в домене (киберпространстве), и во времени. С прикладной точки зрения в нем можно выделить составляющие, тесно связанные с национальной безопасностью, — **военную** и **разведывательную** (к последней примыкают экологический и метеорологический мониторинг, а также ряд конкурентных преимуществ бизнеса и информационное обеспечение средств массовой информации – СМИ). Отдельного внимания заслуживают финансовые аспекты информационного преобладания, которые также могут представлять угрозу международной безопасности.

По нашему мнению, кибероборона США с самого начала строилась не на основе принципов достаточности средств защиты от существующих угроз и балансирования таких

угроз паритетными встречными угрозами, а исходя из целей достижения информационного преобладания, – над любым потенциальным противником.

Такое преобладание предполагалось обеспечить с помощью:

1) достижения проницаемости информационного пространства всех потенциальных противников и заблаговременного выявления любой угрозы своим интересам;
2) формирования стратегического механизма информационного сдерживания (то есть создания с помощью доминирующего кибероружия превентивных угроз, неприемлемых для любого потенциального противника);
3) и повышения уровня защиты собственной информационной инфраструктуры.

Информационное превосходство можно определить как цель информационной войны (либо как основную задачу применения информационного оружия), достигаемую путем «нанесения ущерба информации, процессам, основанным на информации, и информационным системам противника при одновременной защите собственных информации, информационных процессов и информационных систем»[1].

Уместно отметить, что освоение кибернетического пространства военными привело к переоценке многих постулатов военной науки прошлого и представлений о способах обеспечения глобального доминирования.

В самом деле, в современной войне на смену фронтальным сражениям зачастую приходит тактика поражения критически важных объектов противника с помощью бесконтактных боевых действий. При этом важнейшую роль играют информационная составляющая и системы искусственного интеллекта, которые внедрены в технику, высокоточное оружие и другие средства, используемые в рамках единого информационного пространства. Максимально эффективную реализацию их боевого потенциала обеспечивает то, что наиболее целесообразные варианты решения боевых задач, выбор оружия и оценку вероятных последствий удара осуществляет компьютер, обладающий всей необходимой для этого информацией.

Наиболее интересным результатом текущего этапа развития военной стратегии можно считать доктрину «Геоцентрического ТВД» (Geocentric Theter of War, используются также термины Spherical Battlespace и Spherical Area of Operation) предложенную командующим (с января 2011 г. по ноябрь 2013 г.) космическими войсками ВВС США генералом Робертом Келером (Robert Kehler), которому президент Обама в 2010 г. предложил пост шефа Стратегического командования Вооруженными силами США. Келер был назначен на этот пост в январе 2011 г., занимал его до своего выхода в отставку в январе 2014 г. [2]

По мнению автора этой концепции, новый театр военных действий (ТВД) простирается сверху вниз от уровня геостационарной орбиты (примерно 36 тыс. км над Землей) до ее поверхности, последовательно вбирая в себя все арены (домены) военного противоборства — космос, атмосфера, суша, море, а также киберпространство. При этом ключевыми составляющими эффективности использования военной силы являются фундаментальные взаимосвязи космического и кибернетического пространств [3].

Смысл этой концепции заключён в следующих тезисах:

1. Все геоцентрическое пространство (все домены!) представляет собой единую арену военного противоборства.
2. На геоцентрическом ТВД доминируют космические и кибернетические войска, представляющие собой фактически единое целое, а потому действовать они должны под единым командованием.
3. Единство космических и кибервойск обусловлено двумя факторами. Во-первых, быстротечностью операций. Во-вторых, фактическим отсутствием различий между стратегическим и тактическим уровнями управления ими.
4. Последнее означает, что в новой реальности информация, необходимая для управления боевыми действиями, уже не может делиться на тактическую (детальную и локальную) и стратегическую (глобальную, но не столь детальную), как это было

[1] Данное определение присутствует в ряде онлайновых словарей и широко цитируется в Интернете без указания на источник. – *Прим. ред.*

[2] URL: https://en.wikipedia.org/wiki/C._Robert_Kehler.

прежде. На всех уровнях системы управления войсками информационный образ обстановки должен быть одним и тем же – фактически он должен стать «резиновым», его обобщение (агрегирование) недопустимо. Это положение известно как принцип полной ситуационной осведомленности (Situational Awareness).

5. При этом вся информация должна быть и трехмерной, и динамической; любое событие, объект, процесс должны быть локализованы и в пространстве, и во времени.
6. В этой ситуации киберпространство становится не просто средой, в которой противники разрушают сети друг друга, но еще и носителем информационного образа геоцентрического пространства (особой «геоинформационной системой»). Без наличия информационного образа текущей обстановки победа в войне невозможна, а с ним – становится предопределенной.
7. Победа достигается путем заблаговременного выявления угроз и их нейтрализации с помощью концентрации ресурсов – там и тогда, где и когда это необходимо. Таким образом, победа может быть достигнута не путем истощения противника, а с помощью дискредитации его систем управления, иначе говоря, путём его «ошеломления» посредством действий, меняющих обстановку настолько быстро, что тот не успевает уже не только что-либо предпринять, но даже правильно воспринять и оценить происходящее.

Для оперативного освоения этой стратегии Пентагон проводит специальные сетевые игры по обучению военного персонала в режиме реального времени, что должно обеспечить американским военным значительное преимущество в скорости и глубине обоснования принимаемых решений.

Анализ масштабов и содержания проводимых мероприятий, объемы их финансирования и военно-технического обеспечения свидетельствуют о том, что превосходство в информационной сфере рассматривается американским руководством как один из основных факторов достижения целей национальной стратегии в специфических условиях начала XXI века. По определению Пентагона, «превосходство в киберпространстве» означает состояние, когда США и дружественные им силы располагают полной свободой деятельности в киберпространстве, тогда как силы противника такой свободы не имеют. Проще говоря, США исходят из того, что национальных секторов киберпространства просто не существует, а потому никакие государства не могут распространить на них свой суверенитет.

Однако множество обрушившихся на Пентагон кибератак убедило министерство обороны США в том, что американским вооруженным силам необходимы как наступательные, так и оборонительные средства ведения информационной борьбы. Убедительное обоснование направлений деятельности Пентагона в киберпространстве дал заместитель министра обороны США У. Линн III, который в сентябре 2010 г. опубликовал в журнале Foreign Affairs статью «Защищая новое пространство: стратегия кибербезопасности Пентагона» [4].

В этой статье У. Линн III приводит пять основополагающих принципов будущей военной киберстратегии:

- киберпространство должно быть признано таким же пространством войны, как суша, море и воздух;
- любая оборонительная позиция должна выходить за рамки «хорошей гигиены» (пассивной защиты) и включать сложные операции, позволяющие обеспечить оперативное реагирование;
- согласно задачам обеспечения национальной безопасности, кибероборона должна выйти за рамки военных подразделений и распространяться на коммерческие сети;
- для эффективного предупреждения угроз кибероборона должна вестись совместно с зарубежными союзниками;
- министерство обороны должно идти в ногу с развитием индустрии информационных технологий, сохранять и использовать технологическое доминирование США.

У. Линн III отмечает также, что для реализации изложенной стратегии кибероборонны и проведения военных операций в киберпространстве министерство обороны США

изменило свою организационную структуру. Пентагон приступил к созданию надежной многоуровневой обороны военных сетей и возложил ответственность за интеграцию действий по обеспечению кибербезопасности военных компьютеров на новое киберкомандование. (Создание и курирование работы киберкомандования фактически было основным направлением деятельности У. Линна на завершающем этапе его военной карьеры в Министерстве обороны США; его можно считать «отцом-основателем» этой мощной военной структуры).

СОЗДАНИЕ КИБЕРКОМАНДОВАНИЯ

Об усилиях по формированию военного киберкомандования как специальной структуры в рамках Стратегического командования Соединенных Штатов, отвечающей за использование информационно-коммуникационных технологий (ИКТ) вооруженными силами, впервые было объявлено в середине 2008 г. (в конце второго срока полномочий администрации Дж. Буша-мл.). Интересно отметить, что к этому времени в военно-воздушных силах США аналогичная структура уже существовала (она получила обозначение *AFCYBER*). Было объявлено, что киберкомандование *AFCYBER* будет обладать возможностями «сдерживания, разрушения, обмана, разубеждения и поражения врагов при помощи различных средств наступления и обороны» [5].

Несколько позже на авиабазе Лаклэнд в штате Техас было начато строительство первого специализированного кибернетического разведцентра на 400 человек. Это место было выбрано в основном по «географическим» причинам – из-за непосредственной близости к другим подразделениям кибервойск США: разведуправлению ВВС (Air Force Intelligence, Surveillance and Reconnaissance Agency), Техасскому криптологическому центру АНБ, объединенному командованию информационных операций, группе криптологической поддержки ВВС, а также 67-му сетевому крылу космического командования ВВС. Сюда из Сан Антонио была переведена 68-я эскадрилья сетевых операций (68th Network Warfare Squadron) и 710-е звено информационных операций (710th Information Operations Flight). Судя по имевшимся в то время планам, этот специализированный разведцентр должен был работать в основном в интересах космического командования ВВС США.

Проект создания стратегического киберкомандования США при администрации Дж. Буша-мл. реализован не был: во-первых, из-за проблемы определения полномочий вновь создаваемого командования на фоне чрезмерной уязвимости военной инфраструктуры США для внешних кибератак; во-вторых, из-за обострившихся в этот период внутренних противоречий как между родами войск, так и между военными и Министерством внутренней безопасности (МВБ). Дело в том, что создание в составе министерства обороны США организационной структуры по противодействию киберугрозам должно было неминуемо привести к пересечению ее полномочий с полномочиями МВБ. По-видимому, именно эта проблема (помимо прочих) не позволила администрации президента Дж. Буша-мл. создать киберкомандование.

В период второго президентского срока администрации президента Дж. Буша-мл. действия военных по обеспечению безопасности киберпространства проводились плохо скоординированными различными рабочими группами, не связанными друг с другом ни географически, ни организационно. О намерении создать новое военное киберкомандование, призванное обеспечить безопасность не только военных, но и гражданских информационных систем, официальные представители Пентагона объявили только в мае 2009 г. (уже при администрации президента Б. Обамы).

В июне 2009 г. министр обороны США Р. Гейтс, признавая, что потребности в защите киберпространства значительно превосходят имеющиеся в военных структурах возможности, опубликовал меморандум, в котором говорилось об объединении всех рабочих групп под единым командованием – иначе говоря, о создании нового киберкомандования (но не в структуре ВВС, а в рамках Стратегического командования – *STRATCOM*). Такое киберкомандование высшего уровня (*US Cyber Command — USCYBERCOM*) в мае 2010 г. стало составной частью американского стратегического командования [6].

Поначалу на *USCYBERCOM* было возложено три задачи:

1) защита всех военных сетей и поддержка военных действий и операций против кибертеррористов;

2) управление всеми военными киберресурсами и обеспечение соблюдения правил информационной безопасности во всех подразделениях министерства обороны;
3) координация и киберсотрудничество министерства обороны с другими государственными ведомствами, союзниками и частным бизнесом.

При этом продолжали оживленно обсуждаться такие ключевые вопросы, как масштабы вовлеченности государства в обеспечение информационной безопасности, а также полномочия этого нового военного командования. Многие источники сообщали о том, что в перечень функций нового командования будет входить защита не только военных, но и гражданских информационных сетей [7], и выражали обеспокоенность возможной «милитаризацией Интернета».

По мнению ряда экспертов, миссия созданного на стратегическом уровне киберкомандования состоит в «планировании, координации, интеграции, синхронизации и проведении сетевых операций для руководства оборонительными операциями по защите специфических информационных сетей министерства обороны США, а также в подготовке и при необходимости проведении полномасштабных военных кибероперациий во всех доменах в целях обеспечения для США и их союзников свободы действий в киберпространстве и недопущения подобных действий со стороны противника» [8].

Новый импульс созданию военного киберкомандования придал президент Обама, трактуя это событие в контексте реформы общенациональной системы обеспечения информационной безопасности. Эта реформа в целом имела не только военное, но и огромное политическое значение. Ее суть состояла в принятии ряда важных законодательных и организационных мер, направленных на закрепление за Соединенными Штатами статуса глобально доминирующей информационной сверхдержавы, чего невозможно добиться без надежной защиты всех американских пользователей киберпространства. В результате, судя по косвенным данным, более приоритетными были признаны не столько новые технологические возможности ведения наступательных операций, сколько задачи обеспечения информационной безопасности США, и в частности, защиты той части киберпространства, которой пользуется сам Пентагон.

В 2009 г. на слушаниях в Комитете по вооруженным силам Палаты представителей США директор АНБ заявил, что новое командование будет совмещать оборонительные и наступательные информационные средства Министерства обороны и АНБ [9]. Кроме того, посредством создаваемого органа АНБ планирует поддержать министерство внутренней безопасности, в чьи обязанности в настоящее время входит обеспечение информационной безопасности объектов стратегической инфраструктуры Соединенных Штатов.

Согласно официальным информационным материалам «в функции киберкомандования входит подготовка, координация, интеграция, синхронизация действий по проведению операций по защите информационных сетей министерства обороны США, а также, при наличии соответствующего приказа, проведение всего спектра военных информационных операций с целью обеспечения действий вооруженных сил во всех сферах, обеспечение свободы действий американских и союзнических вооруженных сил в киберпространстве, поражение информационных средств противника» [10].

Возглавил новое командование генерал-лейтенант Кит Александер (Keith B. Alexander), сохранивший также за собой пост главы Агентства национальной безопасности (АНБ). Именно на него была возложена ответственность за защиту военных компьютерных сетей и проведение наступательных кибероперациий против вражеских сил. По его мнению, американские военные «должны иметь наступательные возможности, чтобы в режиме реального времени отключать тех, кто пытается на нас напасть» [11].

USCYBERCOM контролировал все ветви американской военной киберсистемы. В его функции входило управление информационными ресурсами министерства обороны, оно объединяет подразделения четырех видов вооруженных сил США: армии (*ARFORCYBER*), авиации (*24th USAF*), флота (*FLTCYBERCOM*) и морской пехоты (*MARFORCYBER*). В 2011 г. в киберкомандовании числилось 931 человек, из которых 464 военных и 467 гражданских лиц, не считая контрактников [12]. В это время министерство обороны США имело в своем распоряжении 15 тыс. сетей и 7 млн компьютерных устройств, размещенных во многих странах мира; их обслуживало более 90 тыс. сотрудников [13].

Использование этого огромного потенциала в военных целях должно было позволить Соединенным Штатам устанавливать в своих интересах информационную блокаду, вести тотальный кибершпионаж, а также «искажать, опровергать, приводить в негодность и уничтожать» информацию и компьютеры по всей планете [14]. Речь идет о том, что с помощью союзников и частных фирм, работающих в сферах информации и безопасности, США планируют установить новый порядок в мировом виртуальном пространстве, что может резко изменить геополитический баланс сил и состояние международной безопасности в целом, а также поставить под сомнение целесообразность многих либеральных достижений информационной эпохи.

СТРАТЕГИИ ПРОВЕДЕНИЯ ОПЕРАЦИЙ В КИБЕРПРОСТРАНСТВЕ

В 2011 г. о своих планах уйти в отставку объявил У. Линн III. До передачи преемнику руководства созданной им структуры он приложил немало усилий для принятия принципиально важного документа – «Стратегии операций МО США в киберпространстве» [15]. (Эта сугубо военная киберстратегия была опубликована всего через два месяца после того, как президент США Обама подписал так называемую «Международную стратегию развития и защиты киберпространства» [16], определившую глобальный – геополитический масштаб американской политики в киберпространстве).

По нашему мнению, именно эта «Стратегия» во многом определила доктринальное содержание подхода министерства обороны США к кибероборонe, превратив кибероружие в самостоятельный силовой фактор современной международной политики.

В ней утверждается, что наиболее серьезные потенциальные угрозы находятся в сфере кибербезопасности, они могут исходить от негосударственных акторов международных отношений. Учитывая роль частного сектора в развитии информационных технологий, негосударственные акторы могут по ряду показателей своего информационного потенциала и информационных ресурсов превосходить некоторые государства. В этом и состоит особенность современной геополитической обстановки, и это очень опасно, поскольку «неудача министерства обороны в обеспечении безопасности своих информационных систем в киберпространстве является фундаментальным риском в отношении его способности выполнять функции обороны страны, как сегодня, так и в будущем» [17].

США категорически отвергают разработку паритетных стандартов международной информационной безопасности (МИБ). В киберпространстве, как и в других сферах внешнеполитического противостояния, они стремятся не просто к новой доктрине (стратегии), о которой уже давно говорят в правительстве [18], а к новому кибероружию, способному обеспечить США реальное доминирование в глобальном информационном пространстве.

Однако упомянутые стратегии оставляют нерешенной проблему направления «ответного удара». В самом деле, если ракета летит из определенного, как правило, заранее разведанного места расположения, то компьютерный вирус может появиться фактически ниоткуда. Из-за огромных объективных трудностей идентификация источника кибератаки в глобальной сети может потребовать времени, несопоставимого с продолжительностью самой атаки. Такая идентификация может затянуться на несколько месяцев или вообще не дать никаких результатов. Здесь важно не забывать, что кибератаки могут осуществляться анонимно, с использованием таких специальных средств, как «анонимайзеры», позволяющих скрыть ее источник, сделать его практически «невидимым» для поисковых систем.

Кроме того, даже если источник кибератаки удалось идентифицировать, его нельзя автоматически считать целью для нанесения ответного удара, поскольку этот источник может принадлежать не государству, а какой-либо независимой группировке, к которой нельзя предъявить какие-либо требования о возмещении ущерба, поскольку у нее нет ни юридического статуса, ни какого-либо имущества. Часто кибератаки исходят из серверов, находящихся в собственности транснациональных организаций (бизнеса) в нейтральных странах.

Более того, не всегда ясно, какой именно киберинцидент можно считать военной атакой. Многие из современных «несанкционированных проникновений» в компьютерные сети являются скорее хулиганством или шпионажем, чем актом войны.

С военной точки зрения Пентагон противостоит только внешней киберагрессии. Поэтому

в документах высокого уровня очень важна явная идентификация неприятеля, что и было сделано в 2011 г., когда впервые главным киберпротивником США был назван Китай [19].

Основное содержание доклада Пентагона, посвященного его политике в киберпространстве и представленного Конгрессу США в ноябре 2011 г., сводится к утверждению о том, что «Соединенные Штаты резервируют за собой право применения военной силы в ответ на любую значительную кибератаку, направленную против американской экономики, правительства или военных... По приказу мы будем отвечать на враждебные атаки в киберпространстве, так же, как мы должны реагировать на все иные угрозы нашей стране. Мы резервируем право использовать для защиты нашей страны, наших союзников и партнеров, а также наших интересов все необходимые средства — дипломатические, информационные, военные или экономические» [20].

Операции в киберпространстве должны проводиться в режиме, подобном традиционным военным операциям. Вместе с тем признается отсутствие исторических прецедентов «традиционной военной деятельности в киберпространстве», а также отсутствие театра (и опыта проведения) такого рода военных действий в период до изобретения современных информационных и коммуникационных технологий, таких как Интернет. Поэтому вопрос о том, могут ли такие операции осуществляться в соответствии с теми же принципами и правовым режимом, которые присущи «кинетическому оружию» и «традиционным военным операциям», требует дополнительного обоснования.

В отношении наступательных операций в киберпространстве, как и в отношении любого иного применения силы должен применяться «Закон о военной силе 93–148» (Public Law 93–148). Признается, что осуществление наступательных операций в киберпространстве в определенном смысле является наиболее эффективным способом противодействия угрозам и защиты вооруженных сил США и их союзников, включая те способы, когда в операциях принимает участие правительство США или когда его роль явно обозначена.

С точки зрения обороны классификация кибератаки противника как значимого события будет осуществляться в соответствие со следующими качественными оценками её последствий: причинение «смерти, ущерба, разрушения или высокого уровня нарушения функций объекта». В соответствии с оценкой уровня последствий, кибератака как значимое событие может повлечь существенный военный ответ, учитывающий размеры нанесенных «потерь».

В декабре 2011 г. Конгресс США санкционировал допустимость военных наступательных операций в киберпространстве [21].

СОВРЕМЕННЫЙ ЭТАП РАЗВИТИЯ ГЛОБАЛЬНОЙ КИБЕРПОЛИТИКИ США

Киберполитика США, направленная на защиту национальных интересов США в международном киберпространстве, изначально носит неравноправный, можно сказать конкурентный характер. Неотъемлемая составная часть американской киберполитики – препятствовать тому, чтобы все остальные страны («партнеры», «конкуренты», «противники») делали то же самое, то есть защищали в глобальной сети свои национальные интересы. Фактически руководство США поставило задачу предотвращения использования глобальной информационной инфраструктуры против интересов США. Это означает лишение конкурентов (не только противников, но и партнеров) даже мизерной возможности сохранять свои коммерческие, научно-технические, политические и прочие секреты, что эквивалентно отрицанию права всех стран мира на сохранение информационного суверенитета.

Нынешний этап эволюции политики США в киберпространстве начался с замены в начале 2014 г. шефа АНБ и *USCYBERCOM* генерала К. Александера на криптолога из ВМС США, адмирала Майкла Роджерса (Michael S. Rogers) [22].

Среди последних документов, подготовленных уже под эгидой нового начальника, можно отметить два – указ президента Обамы ЕО 13694 [23] и новую киберстратегию МО США [24].

Указ был подписан весной 2015 г., он получил название «О блокировке собственности лиц, причастных к значительной враждебной деятельности в киберпространстве». По существу это мера финансового сдерживания, направленная против тех, кто пытается с помощью кибератак нанести ущерб национальной безопасности или экономике США.

Президент объявил, что враждебная деятельность в киберпространстве, осуществляемая из-за пределов США, представляет собой чрезвычайную угрозу национальной безопасности страны. Согласно указу, такая деятельность включает в себя взлом или нарушение работы компьютерных сетей, критической инфраструктуры, а также кражу коммерческой тайны американских компаний или личной информации американских граждан.

В этой связи, вопреки действующим международным нормам, президент наделил министра финансов США правом (по согласованию с генеральным прокурором и госсекретарем) признавать *виновным* в такой деятельности любое иностранное лицо (или организацию), которые, по его мнению, прямо или косвенно к такой деятельности *причастны*, блокировать счета этих лиц (или организаций), а также отказывать им в доступе к находящемуся на территории США имуществу (и отказывать во въезде в США). Более того, согласно этому указу, министр финансов может передать право введения такого рода экономических санкций другим федеральным ведомствам, в том числе силовым.

Фактически этот указ создаёт новую палитру нерыночных методов ведения конкурентной борьбы, с помощью которых правительство США может оказывать давление на зарубежных партнёров в интересах американских компаний.

Одновременно в апреле 2015 г. была представлена новая киберстратегия Министерства обороны США, целью которой было определение направлений развития американского кибероружия, укрепления кибероборонысраны, а также подхода к сдерживанию кибератак. Этот документ сфокусирован на формировании возможностей реализации ряда задач министерства обороны США в сфере кибербезопасности. В новой киберстратегии Пентагона в качестве одной из важнейших задач обозначена защита национальных интересов США от кибератак, «имеющих значительные последствия», и при этом недвусмысленно обсуждаются возможные меры возмездия. (Хотя в Стратегии ещё остаётся некоторая неясность в отношении того, какие случаи Соединенные Штаты будут считать достаточно критическими для немедленного применения намеченных мер возмездия).

ГИГАНТСКАЯ КИБЕРАТАКА

Как бы проверяя решимость администрации Б. Обамы применить в отношении «агрессора» военные или же финансово-экономические меры возмездия, в середине июня 2015 г. международная пресса сообщила о том, что хакеры весь последний год имели незаконный доступ к засекреченным персональным данным 4-х млн действующих и бывших сотрудников силовых и разведывательных служб Соединенных Штатов. В частности, хакеры сумели получить доступ к анкетам и специальным формам № 86, которые американские государственные служащие заполняют при оформлении допусков к секретным работам и сведениям («security clearance»). В этих документах содержится деликатная персональная информация: о болезнях, различных психологических расстройствах, наркотической и алкогольной зависимости человека. Кроме того, в анкетах имелись сведения о кредитной истории, местах прежней занятости, номере соцстрахования, а также контактная информация о ближайших друзьях и родственниках в США и за рубежом [25].

После этой воистину гигантской кражи персональных данных стало ясно, что мер, предпринимаемых в сфере информационной безопасности мало, что, добиваясь транспарентности всего остального мира, США сами остаются весьма уязвимыми для внешних кибератак. Похищение данных миллионов федеральных служащих США обнаружило, что американское правительство десятилетиями пренебрегало безопасностью своих компьютерных систем. Об этом заявила глава Бюро по управлению персоналом (Office of Personnel Management – OMP) Кэтрин Арчулеты (Katherine Archuleta). По ее словам, ущерб от этой хакерской атаки может быть весьма масштабным.

США были первой страной, применившей наступательное кибероружие против суверенного государства (так же, как это ранее было с ядерным оружием и беспилотниками. «Применив столь разрушительные вирусы, как Stuxnet и Flame, Америка сильно подорвала свое нравственное и политическое реноме» [26]. Но теперь Америка сама стала жертвой. И ей надо срочно классифицировать нанесенный ущерб и принять решение об ответных мерах (например, о нанесении ответного кибердара).

После 30-дневного разбирательства в отношении гигантской летней кражи персональных

данных из *OMP*, она была классифицирована как «особый случай», а именно: как беспрецедентный по масштабу шпионаж, который, однако, не был разрушительным и не привёл к краже какой-либо интеллектуальной собственности. Было решено, что возможные негативные последствия этой кибератаки будут нивелированы с помощью существенного усложнения процедур онлайновой идентификации в органах федеральной власти США (в том числе, для привилегированных пользователей).

В самом конце июля 2015 г. газета «Нью-Йорк Таймс» опубликовала весьма содержательную статью своего известного вашингтонского корреспондента Дэвида Сэнджера (David E. Sanger), посвященную последствиям произошедшей масштабной кражи персональных данных государственных служащих США [27].

В статье отмечается, что Соединенные Штаты видят различие между **кибервторжениями**, направленными на нанесение ущерба национальной безопасности (на эти вторжения должна реагировать контрразведка), и **кибератаками**, ориентированными на сбор данных в коммерческих целях (на которые должны реагировать правоохранительные органы). Один из руководителей американской разведки дал понять, что «размеры произошедшего прецедента меняют его природу». Такие прецеденты явно выходят за рамки и уголовных правонарушений, и даже традиционного шпионажа.

Д. Сэнджер обращает внимание на то, что США начали всерьёз обсуждать, как отомстить хакерам, атакующим Америку в киберпространстве на государственном уровне. Так, продолжая идею упомянутого выше указа президента Обамы, адмирал М. Роджерс, совмещающий должности директора АНБ и шефа *USCYBERCOM*, подчеркнул необходимость нанесении «атакерам» (лицам или организациям, ответственным за вторжение) существенного ущерба.

При этом Америка ни с кем не хочет разговаривать «на равных». В статье говориться, что Соединенным Штатам нужно уметь прерывать и сдерживать всё то, что наши враги делают в киберпространстве, и это означает потребность в широкой палитре инструментов обоснования (легендирования) ответных действий.

Кроме того утверждается, что в рамках американского разведывательного сообщества обсуждаются направления поиска ответных операций отмщения. Одним из наиболее «инновационных» направлений назван поиск способов взлома так называемой «великой стены» («great firewall») – комплексной сети цензуры и контроля, которой Китай окружил своё информационное пространство для пресечения диссидентского движения внутри страны. Сама идея такой мести призвана убедить китайских лидеров в том, что, если они не умерят свои атаки на США, они могут лишиться одной из главных внутриполитических ценностей Китая – абсолютного контроля над политическим диалогом в стране.

«СВОБОДА ИНТЕРНЕТУ»

Надо заметить, что идея взлома китайской цензурной стены не нова. Как известно, Америка причисляет свободу Интернета к ценностям высшего порядка, обеспечение которых она относит к своим стратегическим целям. Для достижения этих целей США намерены комплексно использовать все инструменты своей национальной мощи – дипломатические, информационные, военные и экономические, в том числе так называемые факторы «мягкой силы». Одним из наиболее ярких примеров практического использования этих инструментов для защиты «старых ценностей в новых технологических условиях», можно считать соответствующую программу американского Госдепартамента «Свобода Интернету».

Как известно, в странах, практикующих цензуру, граждане нередко лишены доступа к зарубежным мнениям, а также возможностям изложения своей точки зрения. США выступают за то, чтобы всё мировое сообщество «пользовалось в Интернете универсальными правами бесцензурного общения». «Хороших пользователей» (которые не нарушают американских законов) правительство США считает «свободными гражданами, не имеющими национальности и не признающими в глобальном киберпространстве какого-либо государственного суверенитета». Ради защиты их прав США считают возможным вмешиваться во внутренние дела других стран [28].

Составной частью программы «Свобода Интернету» являются проекты создания и распространения специальных онлайновых инструментов (так называемых «анонимайзеров»),

позволяющих обходить сетевые экраны (брандмауэры), которые правительственные органы ряда стран используют в целях контроля (цензуры) национальных сегментов Интернета. (Речь идет о программных кодах, позволяющих пользователям общаться и размещать в сети материалы, направляя свой Интернет-трафик через другие страны и, таким образом, не «засвечиваться» в национальных правоохранительных структурах, то есть сохранять некоторую «анонимность». По мнению специалистов в основу «анонимайзеров» были положены разработки, созданные в рамках известной программы «Tor»).

Программа Госдепа «Свобода Интернету» опирается на идею применения в глобальном киберпространстве универсальных прав доступа к информации». Пользуясь лексикой основателя компании WikiLeaks Джулиана Ассанжа, можно сказать, что США стремятся «распространить на весь мир первую поправку к своей Конституции». В результате любой современный человек должен будет почувствовать себя «Настоящим Американцем» и пользоваться универсальным правом доступа к информации.

Этот тезис полностью соответствует официальной политике «цифровой дипломатии», освещению которой были посвящены два выступления госсекретаря США Хиллари Клинтон в начале 2010 г. (в Вашингтонском «Музее новостей») [29] и в начале 2011 г. (в университете Джорджа Вашингтона) [30].

Вторя знаменитой фултоновской речи У. Черчилля о «железном занавесе», Х. Клинтон заявила, что «распространение практики подобных ограничений во многих странах мира подобно падению информационного занавеса». Эту мысль подтвердил старший советник Х. Клинтон Алекс Росс (Alex Ross): «Мы помогаем людям пользоваться универсальными правами в Интернете. Мы поддерживаем универсальные права, свободу и открытость Интернета» [31].

По данным газеты «Вашингтон Пост», создание и распространение такого рода инструментов оплачивается правительством. Программу «Свобода Интернету» поддерживает лично президент Б. Обама, который заявил об этом на встрече с шанхайскими студентами в 2009 г. [32].

Сегодня, как указывает американская пресса, более 1 млн человек, проживающих в «странах, практикующих цензуру», ежедневно используют онлайновые инструменты, преодолевающие национальные брандмауэры. Финансирование работающих по этому проекту организаций и коммерческих фирм осуществляется по многим каналам, в том числе, Госдепартаментом США, а также Управлением технологий, услуг и инноваций (Office of Technology, Services and Innovation) Совета управляющих вещанием (Broadcasting Board of Governors – BBG) – независимого агентства американского правительства. Директор этого управления Андре Мендес (André Mendes) заявил, что «всякий раз, когда мы предоставляем провайдерам дополнительное финансирование, жесткость цензурных ограничений на время смягчается, однако наши возможности очень быстро исчерпываются» и ситуация возвращается в прежнее состояние. В 2011 г. на эти цели Госдеп выделил около 25 млн долл. По данным же газеты The New York Times, эта цифра – выше 70 млн долл..

АНОНИМАЙЗЕР «TOR»

В этом контексте уместно вспомнить об уникальной квалификации адмирала М. Роджерса, отдавшего более 30 лет своей карьеры военно-морскому флоту США и обладающего не только большим опытом в сфере разведки, но также и опытом руководства «киберфлотом» – специальным киберподразделением ВМФ США.

Это позволяет предположить, что вице-адмирал М. Роджерс имел непосредственное отношение к системе (сети) анонимных пользователей системы Tor, которая была создана разведкой ВМФ США для осуществления специальных операций в киберпространстве, направленных на противодействие авторитарным правительствам, «ограничивающим информационные права граждан».

В 2003 г. проект Tor был рассекречен, переведен в ранг свободного софта и пущен в вольное плавание, а большая часть команды разработчиков плавно перешла из разведывательных структур в специально созданный фонд. При этом эта сеть анонимных пользователей, быстро превратилась в прибежище маргинальных и криминальных киберсубкультур.

Именно эта система в течение первых 2–2,5 лет была основным пространством для обращения новой анонимной виртуальной валюты «биткойн» (после её появления в 2009 г.). При этом

«биткойн выглядел так, будто его создавали в качестве оружия, – написал Чарли Стросс, – призванного нанести удар по центральным банкам в либертарианских целях – помешать государствам собирать налоги и следить за финансовыми транзакциями граждан» [33].

Эта мысль была уточнена в получившей большой резонанс книге двух высококвалифицированных специалистов из «силиконовой долины» Э. Шмидта и Д. Коэна – «Новая цифровая эпоха» [34]. В этой книге при обсуждении способов ослабления «могущества традиционного государства» в цифровую эпоху речь идёт уже не об общих рекомендациях, а о весьма конкретных мерах, например введение «уникальной виртуальной валюты», реализующей в глобальном киберпространстве универсальное право граждан на неконтролируемое государством (анонимное) распоряжение своими деньгами.

Будут ли реализованы глобальные амбиции США – не ясно, уж слишком уязвимыми становятся информационные системы по мере совершенствования технологий. Этот вопрос нуждается в дальнейших исследованиях, в том числе политологических.

US GLOBAL AMBITIONS IN DIGITAL AGE

Evgenii Rogovskii, Doctor of Sci. (Economics),
Head of the Center for Military-Industrial Policy Studies,
Institute for USA and Canada Studies, Russian Academy of Science,
2/3 Khlebny per., Moscow, 123995, Russia.
E-mail: rogowsky@mail.ru

Summary

The article investigates the political problem of U.S. domination in global cyberspace. The author deals with historical questions of U.S. Cybercommand build up and military strategies of cyberwarfare applications. Special attention attracted to political analysis of American information systems vulnerability.

Key words: *information superiority, domination in cyberspace, Pentagon cyberstrategy, "Internet freedom" program, information system vulnerability.*

ЛИТЕРАТУРА /REFERENCES

1. Europe faces a 'real threat' from Russia, warns US army commander. URL: http://www.telegraph.co.uk/news/worldnews/europe/russia/11547247/Europe-faces-a-real-threat-from-Russia-warns-US-army-commander.html
2. URL: http://www.defense.gov/news/newsarticle.aspx?id=45289; URL: https://fas.org/irp/doddir/army/pam525-7-8.pdf
3. URL: http://www.neogeography.ru/ru/2010–05–03–10–15–45/109-sao
4. *Lynn W.*, III. Defending a New Domain: The Pentagon's Cyberstrategy// Foreign Affairs. 2010. Sept./Oct. URL: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain
5. Air Force Cyber Command. «Air Force Cyber Command Strategic Vision». March. 2008. URL: http://www.afcyber.af.mil/shared/media/document/AFD-080303–054.pdf
6. *Miles D.* Gates Establishes New Cyber Subcommand. American Forces Press Service. – Wash. 2009. June 24. URL: http://www.defenselink.mil/ news/newsarticle.aspx?id=54890
7. URL: http://www.washingtonpost.com/wp-dyn/content/article/2009/06/23/ AR2009062303492.html
8. URL: http://rnd.cnews.ru/army/news/top/index_science.shtml?2010/07/09/399982
9. Statement for the Record Lieutenant General Keith Alexander Commander Joint Functional Component Command for Network Warfare before the House Armed Services Committee Terrorism, Unconventional Threats, and Capabilities Subcommittee. 2009. 5 May.
10. US Department of Defense Cyber Command Fact Sheet. 2010. Oct. 13. URL: www.defense.gov/cyber
11. URL: http://fcw.com/Articles/2009/07/06/buzz-cyber-command.aspx?p=1.
12. Statement of General Keith B. Alexander Commander United States Cyber Command Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities. 2011. 16 March.
13. *Daniel L.* Lynn Outlines Cyber Threats, Defensive Measures // American Forces Press Service. URL: http://www.defense.gov/news/newsarticle. aspx?id=60600

14. *Webster S.* Pentagon May Apply Preemptive Warfare Policy to the Internet. 2010. Aug. 29. URL: http://www.rawstory.com/rs/2010/0829/pentagon-weighs-applying-preemptive-warfare-tactics-internet/. (30.08.2010).
15. Department of Defense Strategy for Operating in Cyberspace. –Wash. D. C. 2011. July. URL: http://www.defense.gov/news/d20110714cyber.pdf
16. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. 2011. May. URL: http://www.whitehouse.gov/sites/default/files/ rss_viewer/international_strategy_for_cyberspace.pdf
17. 2010 Quadrennial Defense Review. URL: http://www.defense.gov/qdr /qdr%20as%20of%2029jan10 %201600.PDF
18. URL: http://www.nextgov.com/defense/2010/09/defense-lacks-doctrine-to-guide-it-through-cyberwarfare/47575/
19. Foreign economic collection report 2011. URL: http://www.globalsecurity org/intell/library/reports/2011/foreign-economic-collection_2011.pdf
20. Department of Defense Cyberspace Policy Report to Congress. 2011. Nov. URL: http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934 %20Report_For%20webpage.pdf.
21. Congress Sanctions Offensive Military Action in Cyberspace. 2011. Dec. 15. URL: https://www.infosecisland.com/blogview/18769-Congress-Sanctions-Offensive-Military-Action-in-Cyberspace.html
22. Obama signs off on nomination of Rogers as NSA director. URL: http://www.washingtonpost.com/world/national-security/obama-signs-off-on-nomination-of-rogers-as-nsa-director/2014/01/25/bc54378c-85f7-11e3-801f-e3ff2ca3fab6_story.html?wpisrc=nl_headlines
23. Executive Order 13694 of April 1, 2015 Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities. URL: http://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf
24. URL: http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
25. Chinese hack of federal personnel files included security-clearance database. URL: https://www.google.ru/?gws_rd=ssl#newwindow=1&q=Chinese+hack+of+federal+personnel+files+included+security-clearance+database
26. *Гринуолд Г.* Новое крупное расширение «подразделения кибербезопасности» в Пентагоне предпринято вовсе не ради обороны. URL: http://www.inopressa.ru/article/29jan2013/guardian/cyber.html
27. *Sanger D.A.*"U.S. Decides to Retaliate Against China's Hacking." NYT JULY 31, 2015 URL: http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?hp&action=click&pgtype=Homepage&module =first-column-region&region=top-news&WT.nav=top-news
28. Internet Freedom as a Global Human Rights Issue. URL: http://www.asil.org/ insights120524.cfm
29. *Clinton H.R.* Remarks on Internet Freedom. The Newseum Washington, DC January 21, 2010 www.state.gov/secretary/rm/2010/01/135519.htm
30. Clinton H.R. Internet Rights and Wrongs: Choises & Challenges in a Networked World / George Washington University Washington, DC. February 15, 2011. URL: washingtonpost.com/blog.../clinton_internet_freedom_speec.html
31. ««Мы небудем извиняться за то, что помогаем людям пользоваться универсальными правами». Интервью старшего советника госсекретаря США по инновациям АЛЕКСА РОССА корреспонденту «Ъ» Елене Черненко, Газета «Коммерсантъ», № 172 (4713), 15.09.2011. URL: http://www.kommersant.ru/doc/1773260
32. President Obama at a Shanghai town hall with students, as provided by the White House. URL: http://latimesblogs.latimes.com/washington/2009/11/obama-china-townhall-text.html
33. *Stross Ch.* Why I want Bitcoin to die in a fire. URL: http://www.antipope.org/charlie/blog-static/2013/12/why-i-want-bitcoin-to-die-in-a.html
34. URL: http://www.telegraph.co.uk/technology/internet/10018193/The-New-Digital-Age-by-Eric-Schmidt-and-Jared-Cohen-review.html