ЕЛЕНА ЛАРИНА
ВЛАДИМИР ОВЧИНСКИЙ

КИБЕРВОЙНЫ XXI ВЕКА

О ЧЕМ УМОЛЧАЛ ЭДВАРД СНОУДЕН

Владимир Семенович Овчинский
Елена Сергеевна Ларина

Кибервойны XXI века. О чем умолчал Эдвард Сноуден

Серия «Коллекция Изборского клуба»

Издательский текст
http://www.litres.ru/pages/biblio_book/?art=17071553
Кибервойны XXI века. О чем умолчал Эдвард Сноуден: Книжный мир; М.; 2014
ISBN 978-5-8041-0723-0

Аннотация

Мир на пороге великих перемен, имя которым – Третья производственная революция. И как любая другая революция, эта сопровождается войнами, переделом собственности и сменой господствующих элит. Только это – кибервойны, которые ведутся в Сети кибероружием за господство в будущем кибермире. Сможет ли Россия осуществить прорыв и сотворив «Русское чудо XXI века», занять достойное место в новом, цифровом мироустройстве или потерпит сокрушительное поражение на виртуальных полях сражений незримой Третьей мировой кибервойны и канет в Лету? Будущее покажет.

А каким это будущее может быть, читатель узнает из новой книги эксперта по конкурентной разведке Елены Лариной и известного российского криминолога, генерал-майора милиции в отставке, доктора юридических наук Владимира Овчинского.

Содержание

Введение 6
Глава 1 21
1.1. Феномен кибервойн 23
1.2. История кибервойн 29
1.3. Реалии кибервойн 33
1.4. Факторы угрозы 39
1.5. Великий уравнитель 45
1.6. Неопознанная война: эскалация 50
1.7. На пути к кибермиру 62
1.8. Борясь за кибермир, готовься к новым кибервойнам 66
1.9. Кибероружие сдерживания 73
Глава 2 85
2.1. Взлет и падение «мягкой силы» 88
2.2. Стратегия и тактика превентивных действий 110
Конец ознакомительного фрагмента. 121

Елена Ларина, Владимир Обнинский Кибервойны XXI века. О чем умолчал Эдвард Сноуден

© Е. Ларина, 2014
© В. Овчинский, 2014
© Книжный мир, 2014

Введение
Картография цифровой среды

Цифровая среда включает в себя все многообразие информационных технологий и киберпространство. Киберпространство в строгом смысле этого слова представляет собой ту часть цифровой среды, где происходит управление различного рода объектами физического мира, посредством передачи программ в виде сигналов по Интернету, другим сетям и телекоммуникационным каналам.

Цифровая среда имеет собственные:

• инфраструктуру. Она включает в себя, во-первых, телекоммуникационные и интернет линии (оптоволоконные кабели и т. п.), во-вторых, вычислительные комплексы различной размерности – от суперкомпьютеров до смартфонов и планшетных компьютеров, и, в-третьих, вычислительные управляющие встроенные блоки в различного рода объекты физического мира, начиная от производственных линий, заканчивая кроссовками и майками;

• структуру. Она состоит, во-первых, из сетевых программных протоколов, обеспечивающих передачу информации по различным сетям, включая интернет, корпоративные сети, одноранговые сети (типа Tor) и т. п., во-вторых, программы и программные платформы, осуществляющие

хранение, переработку и представление информации – от баз данных до привычных всем операционных систем, типа Windows, Linux и т. п., и, наконец, в-третьих, программы-интерфейсы, обеспечивающие восприятие информации конечными пользователями (интерфейсы сайтов, блогов, порталов, приложений, различного рода программ и т. п.);

• ультраструктуру. Она представляет собой инфосферу, где содержатся воспринимаемые человеком прямые и скрытые смыслы, выраженные в текстах, таблицах, видео- и аудиоконтенте. Ультраструктура включает в себя, во-первых, общедоступные сетевые ресурсы, типа сайтов, блогов, порталов, социальных сетей и т. п., во-вторых, защищенные, доступные только для определенных категорий пользователей информационные ресурсы государственной и корпоративной принадлежности, в-третьих, общедоступные ресурсы с платным контентом.

За почти 25-летнюю историю развития общедоступных коммуникационных сетей, с 1991 г., когда к закрытой сети получили возможность подключаться все желающие, сложилось два принципиально различных их типа:

• Интернет, а также внутренние государственные и корпоративные сети, недоступные для сторонних пользователей. Эти сети построены по иерархическому принципу. В сетях существует несколько уровней иерархии, которые аккумулируют и передают информацию. Соответственно, права и возможности регулирования информации на каждом уровне за-

висят от его положения в иерархии, чем выше уровень, тем больше возможностей и прав.

• так называемые пиринговые, или одноранговые сети. Наиболее популярные из них в настоящее время – коммуникационная сеть Tor и платежная сеть «Биткойн». В одноранговых сетях информация передается между компьютерами пользователей, которые имеют абсолютно равные права и возможности в передаче информации. Но за равенство надо платить. Поэтому одноранговые сети работают, как правило, медленнее, чем привычный Интернет.

Указанные типы сетей функционируют независимо друг от друга. Соответственно ресурсы одной сети не обнаруживаются и не находятся поисковыми системами другой сети. При этом в каждой из сетей предусмотрены специальные порталы, которые облегчают пользователям использование ресурсов в другой сети.

Интернет имеет следующую картографию:

• web 1. Это наиболее старый, сложившийся сегмент сети. Он включает в себя правительственные, корпоративные, общественные, персональные порталы, сайты, блоги, он-лайн СМИ. Ресурсы этого сегмента сети легкодоступны при помощи поисковых систем (типа Google, Yandex и проч.);

• web 2. Это так называемый социальный веб, или веб социальных сетей и платформ. Здесь расположены такие ресурсы, как «В Контакте», Facebook, Twitter и проч. Контент в этом сегменте интернета создается в основном самими поль-

зователями, поэтому он получил название социального веба. Из-за политики собственников платформ и социальных сетей, а также требований приватности они лишь частично видимы для поисковых систем. В этом сегменте ускоренными темпами растет доля видео- и фотоконтента;

• web 3. Этот сегмент интернета появился в последние 2–3 года и растет наиболее быстрыми темпами. Это так называемый «веб мобильных приложений». Интерфейсы приложений размещаются на экранах планшетных компьютеров, смартфонов. Соответственно пользователи работают с приложениями без обращения к поисковым системам, просто устанавливая связь между своим гаджетом и ресурсом (сервисом, порталом и т. п.) через Интернет;

• невидимый Интернет. Невидимый интернет-это ресурсы, которые не обнаруживаются поисковыми машинами, а также порталы, сайты и т. д., доступ к которым предполагает либо платный характер, либо наличие специального разрешения на использование ресурсов. По имеющимся данным, в невидимом интернете находится порядка 90 % всего ценного научно-технического, технологического, финансово-экономического и государственного открытого контента. Объемы невидимого интернета постоянно растут. Он развивается более быстрыми темпами, чем web 1 и web 2. Главными причинами опережающих темпов являются с одной стороны – стремление к архивации всех доступных данных корпоративными пользователями, а с другой – желание облада-

телей ресурсов вывести их из общедоступного пользования в платный сегмент, т. е. монетизировать.

• интернет вещей. Представляет собой соединенные через интернет с управляющими центрами встроенные информационные блоки самых различных объектов физического мира, в том числе производственной, социальной, коммунальной инфраструктуры. Так, например, к нему относятся подсоединенные к всемирной сети технологические линии, системы управления водо- и теплоснабжением и т. п. Буквально в последние год-два обязательным требованием по умолчанию стало подключение к интернету всех типов домашнего оборудования, бытовой техники, вплоть до холодильников, стиральных машин и т. п.

• бодинет. Со стремительным развитием микроэлектроники появилась возможность встраивать элементы, передающие информацию в предметы гардероба (кроссовки, майки и т. п.), а также широко использовать микроэлектронику в новом поколении медицинской техники, реализующей различного рода имплантаты – от чипов, контролирующих сахар в крови до искусственного сердца и т. п. Кроме того, тенденцией последних месяцев стало создание распределенного компьютера, который предполагает, что отдельные его элементы распределяются по человеческому телу – фактически человек носит на себе компьютер и взаимодействует с ним круглые сутки.

Большую часть одноранговых сетей относят к так назы-

ваемому «темному вебу» (dark web). Своему названию этот сегмент сети обязан широким использованием своих ресурсов различного рода преступными, незаконными группами и группировками. Основными сегментами этого веба являются сеть Tor, созданная в 2002 г. военно-морской разведкой США и платежная сеть «Биткойн». В настоящее время сети используются преимущественно для противоправной деятельности, киберпреступности, торговли наркотиками, оружием и т. п., а также осуществления целенаправленных акций по подрыву государственного суверенитета.

Особый сегмент сети, частично располагающийся в сети интернет, частично – в специально созданных одноранговых сетях, составляет так называемые «сети денег». Общемировой тенденцией является сокращение наличного платежного оборота и переход к электронным деньгам во всех их видах. Сети денег включает в себя специализированные телекоммуникационные расчетные сети, связывающие крупнейшие банки, типа SWIFT, а также платежные системы, использующие интернет, типа PayPal, «Яндекс. Деньги» и т. п. Отдельным, быстро развивающимся сегментом денежных сетей являются специализированные платежные системы, базирующиеся на одноранговых сетях и зашифрованных сообщениях. Наиболее известная из этих систем – это платежная система «Биткойн».

Таким образом, цифровая среда имеет сложную картографию, где отдельные сегменты развиваются по собственным,

независимым от общих закономерностей, трендам. При этом целый ряд основополагающих тенденций являются общими для всех сегментов цифровой среды.

Первой основополагающей тенденцией цифровой среды является информационный взрыв. В последнее время объем информации удваивается каждые два года. По данным компании Cisco объем сгенерированных данных в 2012 году составил 2,8 зеттабайт и увеличится до 40 зеттабайт к 2020 г. Примерно треть передаваемых данных составляют автоматически сгенерированные данные, т. е. управляющие сигналы и информация, характеризующие работу машин, оборудования, устройств, присоединенных к Интернету. На 40 % ежегодно растет объем корпоративной информации, передаваемой и хранящейся в сети Интернет.

Число пользователей интернета в мире к концу 2013 года составило 2,7 млрд, человек, или 39 % населения земли, а к 2016 году эта доля составит 65–75 % населения по данным Центра новостей ООН. Как ожидается, количество корпоративных пользователей Интернета во всем мире увеличится с 1,6 миллиарда в 2011 году до 2,3 миллиарда в 2016 году.

Если в 2012 году более 90 % пользователей выходили в сеть с компьютеров всех типов, и л ишь 10 % – с мобильных устройств, то к 2016 году доля планшетников, смартфонов и других гаджетов увеличится как минимум до 45–50 %.

Россия входит в число ведущих стран по числу пользователей Интернетом. В настоящее время более 55 % населения

взаимодействуете Интернетом. В крупных городах им охвачено более 75 % населения. Происходящее из года в год снижение стоимости широкополосного доступа в интернет, переход на новые стандарты мобильной связи, обеспечение доступа в интернет жителям ранее не охваченных им районов страны, открывают принципиально новые возможности для экономического, общественного и социального развития.

Прежде всего, появляются возможности для создания общегосударственной и корпоративных систем непрерывного дистанционного образования и целевого формировании компетенций по наиболее востребованным, в том числе ранее не существовавшим профессиям и специальностям. Не меньшие возможности открываются перед интернет-медициной, которая в последние несколько лет получила широчайшее распространение в США, Западной Европе, ряде других стран. При этом следует отметить, что в России еще в конце 90-х – начале 2000-х годов в системе РЖД была создана охватывающая всю территорию страны система интернет-медицины, которая с учетом новых технологических возможностей может быть использована как в общегосударственном масштабе, так и в масштабе отдельных регионов, либо крупных корпораций.

Огромные возможности имеются у российской интернет-коммерции. По своим объемам она в 2013 году занимала 13 место в мире. Но по темпам роста она первенствует в Европе. Ключевыми вопросами для устойчивого роста интер-

нет-торговли является опережающее развитие безналичного платежного оборота в виде электронных платежей по кредитным картам и т. п. Развитию российской интернет-коммерции будут способствовать также соответствующие международному законодательству меры по недопущению демпинга со стороны внешних рынков электронной коммерции. Подобные меры в настоящее время действуют в Германии, Великобритании, других странах.

Исторически Интернет формировался как свободная среда информационного взаимодействия при неформальном, но реализованном через жесткие технологические программные и организационные способы контроле со стороны Соединенных Штатов Америки – страны-создателя всемирной паутины. В результате, к настоящему времени сложилось парадоксальное положение. В интернет в значительной степени переместились торговля, финансовые операции, политическая и социальная активность, т. е. ключевые сферы жизнедеятельности каждого государства. Между тем в интернете, в отличие от физической реальности, не признаны поствестфальские принципы международного права. Безусловно, обеспечение «цифрового суверенитета», совместное международное управление интернетом и распространение принципов поствестфальской международной системы на интернет с учетом его особенностей являются важными направлениями внешнеполитической активности России и все большего числа стран, придерживающихся сход-

ных взглядов на принципы международно-правового регулирования Интернета.

Второй важнейшей тенденцией изменения цифровой среды становится формирование Интернета вещей. Интернет вещей – это самые разнообразные технологические, производственные, инфраструктурные устройства, приборы, приспособления и т. п., имеющие блоки контроля, передачи информации и управления, соединенные с интернетом. В настоящее время к интернету уже подключено более 17 млрд, устройств.

Согласно сделанному IDS прогнозу к интернету вещей к 2020 году будет подключено 212 миллиардов устройств, а денежная ёмкость этого рынка I составит 8,9 трлн, долларов. Причём в интернете вещей образца 2020 года окажется 30,1 млрд, автономных устройств, от автомобилей до пылесосов.

Развитие интернета вещей открывает поистине безграничные перспективы и возможности для российской и мировой экономики. Анализ данных, поступающих от соединенных с интернетом инфраструктурных объектов, позволяет, как показывает мировой опыт, на 20–30 % сократить время, проводимое на перегруженных автомобильных трассах, более чем на 15 % сократить непроизводительные расходы воды и электроэнергии в жилых и производственных зданиях и т. п. Как свидетельствует опыт Финляндии и Норвегии, использование технологии «умных домов» и «умных

кварталов», предусматривающей, в том числе подсоединение к интернету системы как поквартирного, так и централизованного тепло- и энергоснабжения позволяет на 12–17 % уменьшить расходы на отопление при сохранении неизменной температуры в жилых помещениях. Понятно, что в условиях нашей страны использование интернета вещей в подобных сферах даст еще более впечатляющий эффект. Этот эффект может быть связан, во-первых, с природно-климатическими особенностями нашей страны, во-вторых, со значительным отставанием реализации программ экономии различных, в том числе, коммунальных ресурсов, и, в-третьих, с достаточным и все возрастающим количеством мегаполисов и агломераций, где он проявляется наиболее сильно и масштабно.

Как правило, угрозы, связанные с интернетом вещей сводят к различным видам киберпреступности и даже к кибертерроризму. Понятно, что в условиях, когда вся инфраструктура населенных центров, отдельных жилых кварталов, домов и просто жизнедеятельности каждого человека полностью завязана на интернет вещей, злонамеренное вторжение в Интернет вещей может привести к трудно предсказуемым последствиям. Поэтому первостепенной задачей государств с высоким уровнем интернетизации населения и доходов, позволяющих приобретать предметы со встроенным интернетом, становится налаживание теснейшего международного сотрудничества по борьбе с киберпреступностью и

кибертерроризмом. Причем, уже сегодня ясно, что это сотрудничество не должно ограничиваться принятием соответствующих юридических актов, но и должно предполагать каждодневный обмен информацией и эффективным инструментарием борьбы против киберпреступности и кибертерроризма. Более того, заслуживает внимания предложение о создании объединенных добровольных международных сил по противодействию трансграничным киберпреступным и кибертеррористическим группировкам. Россия, располагающая первоклассными специалистами и имеющая целый ряд компаний-резидентов, являющихся лидерами в сфере индивидуальной и корпоративной информационной безопасности, несомненно, может сыграть в этой работе заметную роль.

Существует еще одна в должной мере неосознаваемая угроза цифровому суверенитету России, связанная с интернетом вещей. В настоящее время поисковые системы и платформы социальных сетей, такие, как Facebook, Twitter и др. позволяют анализировать поведение пользователей, объединяемых в самые различные группы, их предпочтения, активности, связи и т. п. С появлением интернета вещей такой мониторинг в режиме он-лайн может вестись уже не в отношении интернет-активности, а в отношении реальной жизнедеятельности населения, функционирования предприятий, организации работы городских и иных структур. Дело в том, что в рамках интернета вещей информация передает-

ся в компании-производители изделий, соединенных с интернетом, либо, в компании-поставщики чипов, микропроцессоров. Соответственно именно в этих компаниях, наряду с индивидуальными, корпоративными или государственными пользователями систем, оснащенных интернетом вещей, оказывается полная информация о реальном мире в режиме он-лайн. Именно поэтому ведущие интернет-компании, например, Google начали заключать сделки ценой от сотен до миллиардов долларов по приобретению компаний, связанных с интернетом вещей. Этой угрозы можно избежать двумя способами. Радикально – развив собственную микроэлектронную промышленность, производящую чипы для приборов, оборудования и систем, подсоединенных к интернету вещей. Паллиативно, установив в качестве обязательного условия для продажи на территории РФ предметов, оборудования и устройств, подключенных к интернету, наличие на территории РФ и подпадающих под его юрисдикцию центров обработки данных (ЦОД) соответствующей компании.

Буквально на наших глазах рождается нательный, носимый интернет, или как его еще называют «бодинет». Этот фрагмент сети складывается из трех сегментов. Прежде всего, появились уже первые предвестники эры распределенных компьютеров, типа очков Google Glass. Вторым сегментом являются предметы гардероба, т. е. повседневная одежда, обувь и т. п., соединенная с интернетом и контролирующая, как правило, состояние здоровья или иных парамет-

ров обладателя гардероба. Наконец, наиболее активно в перспективе будет развиваться сегмент, связанный с электронными компонентами микроустройств и микроприспособлений, непосредственно имплантированных в тело человека. Так, на сегодняшний день уже около миллиона американцев имеют медицинские имплантаты, подсоединенные к интернету, в основном связанные с кардиоконтролем, а также контролем за состоянием сахара в крови. Ежегодно цена на такого рода имплантаты падает не на проценты, а в разы. Также по экспоненте увеличивается количество такого рода имплантатов, в значительной мере порожденных достижениями биотехнологий и микроматериаловедения. Есть основания полагать, что в ближайшие 5–7 лет встроенные в человеческое тело имплантаты, соединенные с интернетом, из экзотики превратятся в обыденность практически во всех развитых странах мира.

При общем отставании в лечебном, в том числе коммерческом использовании такого рода имплантатов, российские исследователи имеют целый ряд впечатляющих разработок и в целом входят в число мировых лидеров в сфере медицинских кибертехнологий. Соответственно при должной организации взаимодействия частного бизнеса и государства в этой сфере отечественный высокотехнологичный бизнес не только может сохранить за собой значительную долю внутреннего рынка, но и имеет хорошие шансы выдержать конкуренцию в отдельных сегментах глобального рынка высо-

ких медицинских интернет-технологий.

Широкое распространение бодинета порождает принципиально новые типы угроз, связанные с возможностью осуществления киберпреступлений, вплоть до нанесения тяжелых телесных повреждений и убийств, а также целевого точечного кибертерроризма. В Соединенных Штатах данная угроза рассматривается как актуальная, и как на государственном уровне, так и на уровне частных компаний разрабатываются конкретные меры по противодействию ей. Принимая во внимание признанную во всем мире высочайшую квалификацию российских специалистов в сфере тестирования на несанкционированное проникновение (этичные хакеры) есть отличный шанс превратить угрозу в возможность для российского бизнеса, и опосредованно для российского государства. Для реализации этой возможности надо в кратчайшие сроки выступить с российской частно-государственной инициативой на международной арене по созданию единого пула производителей медицинских имплантатов, микроэлектронной техники и компаний в сфере информационной безопасности и тестировании несанкционированного проникновения. Такой пул может в перспективе стать надежным щитом для массовой киберпреступности, связанной со злонамеренным вмешательством в работу имплантатов, соединенных с интернетом.

Глава 1
Кибервойны XXI века

В выступлении на Генеральной Ассамблее ООН, посвященном событиям в Сирии, Барак Обама сказал об исключительности Америки и ее праве на военное насилие: «Я считаю, что Америка – исключительная страна: отчасти потому, что все видели, как мы проливаем кровь и не жалеем средств, отстаивая не только свои узкие интересы, но также и всеобщие интересы… Будут ситуации, когда международному сообществу придется признать, что во избежание наихудшего развития событий может потребоваться многостороннее военное вмешательство». Такой подход несомненно еще более дестабилизирует и без того сложную международную геополитическую обстановку и толкает цифровой мир к эпохе кибервойн.

Реально ведущаяся кибервойна, воспринимаемая до последнего времени некоторыми политиками и аналитиками и в России, и за рубежом как некая экстравагантная тема, приобрела в августе 2013 года реальное воплощение. Связано это с документами, которые оказались доступными для журналистов и аналитиков, благодаря Эдварду Сноудену. Речь идет отнюдь не о программах Prism и XKeyskore, или тотальной прослушке мобильных операторов, и даже не о доступе

АНБ к серверам Google, Microsoft, Facebook, Twitter, международной сети банковских транзакций SWIFT, процессинговым система Visa, MasterCard и т. п.

Самыми интересными и пока недостаточно оцененными стали документы в составе досье Сноудена, получившие название – «файлы черного бюджета американского разведывательного сообщества». Российские СМИ, да и экспертное сообщество ограничились обсуждением 231 наступательной кибероперации и броской цифры – 500 млрд, долларов расходов на разведку в США за 2001–2012 гг.

Эти документы, опубликованные газетой Washington Post, дают большую пищу для по-настоящему серьезного анализа. В отличие от слайдов презентаций и мало кому интересных списков IP адресов, аналитики получили в свое распоряжение множество сухих бюджетных цифр и сопровождающие их пояснительные документы, излагающие бюрократическим языком факты, замечания и предложения, касающиеся настоящих, а не медийных секретов американской разведки и армии.

Анализ этих документов позволяет сделать вывод, что в мире уже ведется необъявленная крупномасштабная цифровая, или кибервойна. Единственно остающийся вопрос: когда в этой войне появятся первые человеческие жертвы и масштабные разрушения крупных материальных объектов?

1.1. Феномен кибервойн

Термин «кибервойны» прочно вошел не только в лексикон военных и специалистов по информационной безопасности, но и политиков, представителей экспертного сообщества. Он стал одним из мемов, активно поддерживаемых и распространяемых СМИ всех форматов. Более того, кибервойны стали одной из наиболее обсуждаемых тем в социальных сетях, на интернет-площадках и т. п.

Между тем, существует достаточно серьезное различие в понимании кибервойн, что называется на бытовом уровне и в популярных СМИ, и определением кибервойн профессионалами информационной безопасности и военными.

Среди политиков, медиатехнологов, в СМИ весьма популярна расширительная трактовка кибервойн. Фактически, под ними понимается любое противоборство в кибер- или интернет-пространстве. Некоторые специалисты и эксперты к кибервойнам относят многоаспектные и сложные информационные компании, нацеленные на изменения ценностных ориентаций, политических предпочтений, а иногда даже культурных кодов. Наконец, в разряд кибервойн попадают и репутационные войны, которые ведутся между различными бизнес-группами, компаниями, корпорациями, получившие название «войн брендов».

Такое понимание связано в значительной степени с исто-

рией развития информационных технологий вообще и интернета в частности. Первоначально в лексикон военных вошел термин «информационная война». Его ввела в оборот корпорация RAND в 1990 г. Чуть позднее ведущий сотрудник этой корпорации Мартин Либитски опубликовал книгу «Что такое информационная война». Примерно 10 лет его точка зрения была общепринятой. По М. Либитски эта война имеет семь типов: командно-управляемый, разведочный, психологический, хакерство, экономический, электронный и киберборьба. Свою точку зрения автор продолжает отстаивать до сегодняшнего дня. При этом, несомненное первенство он отдает психологическому воздействию, в первую очередь, дезинформации, PR-компаниям и специальным информационным операциям.

Однако с активным развитием информационных технологий возникла естественная потребность вычленять из общего отдельные направления. Впервые это было сделано американскими военными Джоном Аркуилла и Дэвидом Ронфилдом в статье «Cyberwar is Coming!», опубликованной весной 1993 г. в одном из ведущих журналов американских вооруженных сил Comparative Strategy (т. 12, № 2). В сфере информационной безопасности термин «кибервойны» стал широко использоваться с 2007 г.

С конца первого десятилетия нынешнего века четкое разделение информационных и кибервойн стало общепринятым стандартом для военных, специалистов в сфере инфор-

мационных технологий и информационной безопасности. В первую очередь это произошло в тех странах, которые оказались во главе начавшейся гонки кибервооружений, прежде всего США, Китая, Израиля и т. п.

В то же время в России некоторые аналитики продолжают отождествлять информационные и кибервойны. Они рассматривают их, прежде всего, под углом зрения воздействия информационных потоков на коллективную психику и сознание человека. Такая спутанность понятий, объяснимая в первую очередь текущей политической ситуацией и историей нашей страны, несомненно, повлияла на то, что Россия, обладая огромным потенциалом в сфере информационных технологий, должным образом не оценила опасности, риски и угрозы, связанные именно с кибервойнами.

Информационные и кибервойны разделяются по объектам и средствам боевого воздействия.

Информационные войны – это контентные войны, имеющие своей целью изменение массового, группового и индивидуального сознания, навязывание своей воли противнику и перепрограммирование его поведения. В процессе информационных войн идет борьба за умы, ценности, установки, поведенческие паттерны и т. п. Информационные войны велись задолго до интернета, насчитывают историю, измеряемую даже не сотнями, а тысячами лет. Интернет просто перевел эти войны на качественно иной уровень интенсивности, масштабности и эффективности. Объектом воздействия

информационных войн являются самые различные субъекты – от небольших групп до целых народов и населения целых стран. Средством боевого воздействия являются специально созданные семантические сообщения в виде текстов, видео- и аудиорядов, рассчитанные на восприятие сознанием, обработку мышлением и эмоциональный отклик со стороны групп различной размерности.

Что же касается кибервойн, то это целенаправленное деструктивное воздействие информационных потоков в виде программных кодов на материальные объекты и их системы, их разрушение, нарушение функционирования или перехват управления ими.

Бывший высокопоставленный чиновник, а ныне эксперт по безопасности Правительства США Ричард А. Кларк в своей книге «Кибервойна» (2010 г.) дал такое определение: «Кибервойна – это действие одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения».

Генеральный Секретарь ITU Хамадун И.Туре в докладе «В поисках кибермира», опубликованном в 2012 г., писал: «Понятие кибервойны охватывает не только опасности для военных систем и средств, но также и для жизненно важной общественной инфраструктуры, включая интеллектуальные энергосети, сети диспетчерского управления и сбора данных SCADA, которые позволяют им работать и осуществлять са-

мозащиту».

По де-факто сложившемуся, но юридически не закрепленному мнению подавляющего большинства военных и специалистов по информационной безопасности (вне зависимости от их страновой принадлежности), под кибервойнами понимаются целенаправленные действия по причинению ущерба, перехвату управления или разрушению критически важных для функционирования общества и государства сетей и объектов, производственной, социальной, военной и финансовой инфраструктуры, а также роботизированных и высокоавтоматизированных производственных, технологических линий. Средством боевого воздействия в кибервойнах является программный код, нарушающий работу, выводящий из строя, либо обеспечивающий перехват управления различного рода материальными объектами и сетями, оснащенными электронными системами управления.

Информационные и кибервойны представляют собой две разновидности войн, ведущихся в сетевом электронном пространстве, которое охватывает не только интернет, но и закрытые государственные, военные, корпоративные и частные сети. Для каждого из этих двух типов войн свойственны свои инструментарии, методы, стратегии и тактики ведения, закономерности эскалации, возможности предупреждения ит.п.

Кибервойны тесно связаны с кибершпионажем, киберпреступностью и кибертерроризмом. При этом, необходимо

подчеркнуть, что также как и в материальном мире, в электронном пространстве все эти феномены тесно переплетены и взаимодействуют между собой. Это взаимодействие характерно как для взаимной переплетенности атакующих субъектов, так и объектов, подвергаемых атакам. Эти виды преступного поведения используют зачастую схожие программные средства, имеют сходные режимы их применения и т. п.

Есть все основания полагать, что в течение ближайших двух-трех лет сформируются инструментарии и технологии для электронных войн третьего типа, в каком-то смысле объединяющих информационные и кибервойны. Речь идет о том, что в лабораториях уже прошли практическую апробацию аппаратные и программные средства, обеспечивающие прямую и обратную связи между изменениями психики, или как еще говорят идеального или субъективного, и преобразованием реального мира, соответственно, материи, материальных объектов, их систем, сетей и т. п. Первые публикации на этот счет появились в США и России в этом году. В них говорится о пси-войнах, нейровойнах и т. п.

1.2. История кибервойн

Как известно, история в современном мире является в значительной степени инструментом информационного противоборства. Не избежала этой доли и весьма короткая история кибервойн. Например, в электронном журнале «Вестник НАТО», в статье «История кибератак: хроника событий» история кибервойн начинается с якобы имевшей место в апреле 2007 г. атаки на эстонские государственные сайты и сети со стороны неизвестных иностранных злоумышленников. Вторым ключевым событием кибервойн журнал считает взлом и вывод из строя иностранными злоумышленниками Интернет-сетей в Грузии в августе 2008 г.

При этом и в первом и во втором случаях, вне зависимости от их реальности имели место кибератаки, никак не связанные с нарушением работы критически важных инфраструктурных сетей и объектов. В этом смысле четкое понимание кибервойн, как воздействия из киберпространства на материальные объекты, сети, системы является чрезвычайно важным.

Исходя из этого, большинство экспертов считает, что установленные случаи использования кибероружия, т. е. фактически кибервойны, связаны с деятельностью Соединенных Штатов и Израиля. А в части кибершпионажа несомненное первенство держит Китай.

Первое задокументированное использование кибероружия в ходе крупномасштабных военных действий связано с применением программ, блокирующих работу сирийских ПВО и радиоэлектронной разведки во время проведения так называемой операции «Оливы» в 2008 г.

Масштабное применение кибероружия впервые имело место по данным «Лаборатории Касперского» в Иране в 2010 г. В отличие от обычных вредоносных программ, работающих в популярных операционных системах, примененный против Ирана вирус Stuxnet был специально создан для проникновения в автоматизированные системы, регулирующие и управляющие определенным типом оборудования, связанным с конкретными технологическими цепочками в атомной промышленности. Первоначально никто не брал на себя ответственность за создание и использование этого вируса, однако, не так давно американские официальные лица подтвердили, что он был создан в системе АНБ с участием израильских компаний для противодействия иранской атомной программе. Еще более сложная, многокомпонентная боевая программа была применена американцами и израильтянами против нефтяных терминалов и нефтеперерабатывающих заводов все того же Ирана.

Кроме того, были зафиксированы случаи использования компьютерных вирусов для вывода из строя систем SCADA крупнейшей саудовской нефтяной и катарской газовой компаний.

Серьезным уроком краткой истории кибервойн является тот факт, что некоторые страны быстро поняли, что кибероружие является дешевым и эффективным способом противодействия высокотехнологичным вооружениям. Характерным примером использования кибероружия является перехват системы управления новейшим американским беспилотником и его принудительная посадка на территории Ирана.

По данным ведущих компаний в сфере информационной безопасности в последние год-два наблюдается буквально эскалация кибервооружений. В последнее время были обнаружены такие многофункциональные программы слежения, шпионажа и доставки боевых вирусов, как Flame и Jaiss. По мнению «Лаборатории Касперского», поддержанному крупнейшими экспертами самых различных стран, разница между Stuxnet и обнаруженными новыми многофункциональными программами кибервойны примерно такая же, как между рядовым эсминцем и самым современным авианосцем.

Еще одним уроком кибервойн является тот факт, что согласно данным печати и отдельным отрывочным заявлениям официальных лиц, над этими и другими видами кибервооружений в виде целевых вирусов и многофункциональных программ непосредственно трудились частные компании, а иногда даже группы специально нанятых хакеров. Такой подход полностью соответствует принятому, например, США активному привлечению частных компаний к выпол-

нению функций внутри военных и разведывательных структур. Подобная тактика позволяет государствам отмежевываться от актов киберагрессий и кибертерроризма.

В этой связи наводят на размышления факты, всплывшие в ходе скандала со Э. Сноуденом. Например, выяснилось, что, в АНБ до 70 % не только исследовательских, но и текущих оперативных работ выполняется частными подрядчиками. По имеющимся данным такая же картина характера для Великобритании, Израиля и ряда других стран.

1.3. Реалии кибервойн

Короткая история киберагрессий, а также анализ кибершпионажа и крупномасштабной киберпреступности дают достаточно материалов для выделения основных черт кибервойн, в корне отличающих их от всех других типов военных действий.

Прежде всего, несомненным является высокий уровень анонимности кибервойн. Он связан с трудностями определения киберагрессора. Частично эти трудности сопряжены с самой природой кибервойны, как воздействий в системе компьютер/компьютер через многослойные и запутанные сети электронных коммуникаций. Кроме того, имеются многочисленные, постоянно совершенствующиеся программные средства установления помех, затрудняющих обнаружение хакерских программ, находящихся на вооружении боевых подразделений, разведывательных структур и преступных группировок. Достаточно привести пример крупнейшей кибершпионской сети Red October, которая беспрепятственно действовала в киберпространстве с 2007 по 2012 гг., когда не без труда была обнаружена экспертами «Лаборатории Касперского».

Поскольку между шпионским и боевым софтом нет принципиальной разницы, за исключением функционала основной программы (в первом случае, нацеленной на выкачива-

ние файлов из различного рода сетей и ресурсов и отслеживание действий на компьютерах пользователей, а во втором случае – на разрушение/перехват подсистем автоматического управления теми или иными объектами или сетями), то приведенный пример является весомым аргументом в пользу высокой степени анонимности кибервойн.

Другой отличительной особенностью кибервойн является неопределенность времени их начала. Все привычные человечеству виды войн начинались с хорошо фиксируемых материальных действий и соответственно имели четкую временную привязку. Многокомпонентные программы, как основное оружие кибервойн, могут проникать в сети и управляющие системы разнообразных военных и гражданских объектов и инфраструктур заблаговременно. В этом случае фактическим началом войны будет проникновение этих программ в сети, а фиксируемым моментом начала боевых действий станет активация указанных программ в целях разрушения, либо перехвата управления над инфицированными сетями и объектами.

Уникальной особенностью кибервойн является их потенциальная бесследность. Любое известное вооружение имеет ярко выраженные признаки применения, которые позволяют с уверенностью говорить о начале, ходе и последствий военных действий. Хорошо известно, что с первых дней разработки различного рода хакерского софта одной из главных задач было обеспечение необнаруживаемости последствий

его использования. В этом направлении, как свидетельствует практика незаметного преодоления систем информационной безопасности как крупных корпораций, так и государственных сетей различных стран, достигнуты большие успехи. Соответственно, очевидно, что при разработке боевого софта особое внимание будет уделяться маскировке последствий его использования под имитацию обычных технических отказов, сбоев в работе, либо последствий ошибок со стороны обслуживающего персонала. По мнению и российских, и зарубежных экспертов в области информационной безопасности, все необходимые предпосылки для решения подобных задач имеются уже на сегодняшний день.

Еще одной отличительной чертой кибервойн является отсутствие в этих войнах таких привычных понятий, как «фронт», «тыл». Фактически в кибервойнах потенциальным фронтом, т. е. местом боевых действий являются любые – и военные, и гражданские компьютерные сети и завязанные на них объекты и инфраструктуры.

Следует честно признать и такую крайне неприятную черту кибервооружений, как чрезвычайная сложность их контроля со стороны государственных систем разведки и безопасности. Как полагают многие специалисты, в наиболее изощренных вариантах по своим последствиям кибероружие сравнимо с применением ядерных боевых зарядов. В этом плане есть смысл сравнить возможности контроля над боевым софтом и производством ядерных вооружений. Как

известно из многих отчетов на эту тему, насчитывается около 50 перекрестно подтвержденных случаев попыток завладения расщепляющими материалами, либо технологиями, связанными с производством атомного оружия со стороны террористических группировок и государств, не обладающих атомным оружием. Все подобные попытки были пресечены, поскольку спецслужбы уже давно научились контролировать трафик радиоактивных материалов, отслеживать производителей соответствующего оборудования и выявлять логистику практически в режиме реального времени.

Прямо противоположная ситуация складывается с контролем за производством боевого софта. Главное, что требуется для его изготовления – это высококвалифицированные программисты и аппаратная часть, которая может быть собрана своими силами из комплектующих, массово продаваемых на открытом рынке. Отследить таких производителей является крайне сложной задачей. Разработка боевого софта сегодня доступна не только для государств и крупных корпораций, но и для небольших, хорошо финансируемых групп. А деньги, как хорошо известно, являются едва ли не самым малодефицитным ресурсом в современном мире. Практическим доказательством данного тезиса являются многочисленные факты вывода из строя (либо задание ложных целей) путем целенаправленного программного воздействия американских вооруженных беспилотников в ходе боевых действий в Афганистане.

Наконец, нельзя не сказать о такой отличительной черте кибервойн, как отсутствие для них каких-либо рамок международного регулирования. На первый взгляд на такие рамки может претендовать так называемое Таллиннское руководство по ведению кибервойны (The Tallinn Manual on the International Law Applicable to Cyber Warfare). Однако Руководство не является официальным документом ни НАТО, ни стран, которые входят в НАТО. Это всего лишь частная точка зрения участников рабочей группы, которая написала Руководство в значительной степени в методологической и учебных целях.

Как правило, отсутствие правового регулирования кибервойн связывают с непроработанностью юридических аспектов вследствие новизны вопроса. Однако, на наш взгляд, проблема гораздо глубже и серьезнее. На сегодняшний день интернет управляется организацией ICANN, фактически подконтрольной США и ее ближайшим союзникам. Однако в самые последние месяцы в значительной степени под воздействием разоблачений Эдварда Сноудена даже ближайшие союзники США в Европе, Латинской Америке, Азии требуют интернационализации управления интернетом. В частности, это нашло свое отражение в документах состоявшейся в 2013 г. в Монтевидео очередной конференции ICANN. На этой конференции было принято решение дистанцироваться от Правительства США и вывести всех его представителей из руководящих органов ICANN.

Важно, что регулирование осуществляется в рамках парадигмы «один мир – один интернет». При таком подходе вообще невозможны какие-либо привычные в военном праве межгосударственные соглашения. Дело в том, что ICANN отрицает право государств так или иначе регулировать, а значит, и нести ответственность за тот или иной сегмент интернета. Таким образом, имеет место парадокс. Де факто интернет и другие сети имеют наднациональный характер, а боевые действия в киберпространстве ведутся в отношении конкретных национальных государств и их структур. В рамках сложившейся ситуации, никакие юридические, и шире – согласительные механизмы профилактики и предотвращения кибервойн просто не могут действовать.

Таким образом, приведенные характерные черты кибервойн позволяют сделать вывод об их уникальности относительно всех других типов военных действий. Эти же свойства делают кибервойны особо опасными, легко развязываемыми и трудно урегулируемыми.

1.4. Факторы угрозы

Тенденции технологического развития, темпы и противоречивость мировой динамики являются дополнительными дестабилизирующими факторами. Эти факторы повышают вероятность, расширяют масштабы и увеличивают разрушительную мощь применения кибероружия.

Экспоненциально растет интернет вещей. Уже сегодня он включает в себя не только бытовую технику и даже предметы гардероба, но и «умные» дома, кварталы и города, где практически все сети и предметы имеют встроенные, либо удаленные системы автоматизированного контроля и управления, подключенные к интернету. Сегодня большинство IP адресов принадлежат не пользовательским и корпоративным устройствам и сетям, а также Интернет-ресурсам, а промышленным, инфраструктурным объектам, а также системам управления вещами и сетями, буквально окружающими современного горожанина. Согласно данным компании Cisco, уже в настоящее время на интернет вещей приходится 10 млрд. IP адресов, а в 2020 г. число таких адресов возрастет не менее чем до 50 млрд.

По оценкам ведущей аналитической компании Neilsen, уже сегодня интернет вещей берет на себя более 70 % интернет-трафика. По сути, всеобщая интернетизация вещной среды, окружающей человека, как на производстве, так и в

быту крайне обостряет проблему информационной безопасности, поскольку многократно увеличивает количество взаимодействующих сетей. В условиях, когда даже крупнейшие государственные сети практически ежемесячно оказываются жертвами хакеров, ожидать, что будет обеспечена должная защита всех компонентов интернета вещей, было бы утопией. По данным компании Symantec, производителя линейки программ Norton, в настоящее время не более 3 % вещей, имеющих выход в интернет, имеют хотя бы минимально допустимый уровень информационной безопасности. Для боевых программ интернет вещей является едва ли не самым уязвимым сегментом электронных коммуникаций.

Буквально на наших глазах, вслед за интернетом вещей появился так называемый «бодинет». Он включает в себя миниатюрные электронные устройства, используемые в диагностических, лечебных целях, а также во все ширящихся системах прямого интерфейса компьютер-человек. Первой ласточкой такого рода интеграции являются уже поступившие в продажу так называемые очки Google Glass. По оценкам экспертов, в течение ближайших двух-трех лет успехи нанотехнологий позволят создать массовые продукты на основе контактных линз, имплантированных контрольных чипов для людей с хроническими заболеваниями и т. п. Уже в этом году только в Соединенных Штатах будет продано более 12 млн. индивидуальных медицинских приборов, приспособлений и имплантатов, подключенных к интернету.

Как правило, такие системы имеют единые пункты контроля и управления в компаниях-изготовителях. Причем, взаимодействие между микроустройствами на теле, либо в теле человека и управляющим центром опять же осуществляется по интернет-линиям. Это не фантастика. В этом году в Соединенных Штатах уже вынесен приговор, связанный с убийством посредством отключения кардиостимулятора, параметры работы которого контролировались через интернет. Развитие бодинета, несомненно, открывает новые горизонты, прежде всего, для кибертерроризма и специальных операций в ходе кибервойн.

Невиданные ранее чрезвычайно благоприятные для применения кибервооружений, кибертерроризма и кибершпионажа возможности открывает уже совершившийся переход к множественности подключений к общедоступным и внутренним сетям с одного устройства. До взрывного роста мобильного интернета с практически полным охватом населения развитых стран мира такими устройствами, как планшетники, смартфоны и т. п., была возможность решать проблему информационной безопасности за счет размежевания общедоступных и внутренних сетей аппаратным способом. Грубо говоря, одни компьютеры предназначались для дома или работы в открытых сетях, а другие, не связанные с интернетом компьютеры, функционировали в составе закрытых, высокозащищенных сетей. На сегодняшний день имеются уже не сотни, а тысячи примеров, когда несмотря на

все увещевания специалистов по информационной безопасности, работники самого разного ранга, как в государственном (в том числе военном) секторе, так и в частных компаниях используют одни и те же мобильные устройства для работы со множеством сетей, и в первую очередь с общедоступным интернетом.

Свою лепту в создание дополнительных угроз вносит и активное развитие облачных вычислений. Облачные вычисления делают доступными для бизнеса, государственных структур наиболее дорогостоящие и сложные программные продукты, обеспечивают значительную экономию на развертывании аппаратной и программной частей IT инфраструктуры, содержании высококвалифицированных системных администраторов и т. п. Но их экономические достоинства могут обернуться существенными проблемами в сфере информационной безопасности. Облачные технологии априори предусматривают, особенно в корпоративном секторе, наличие множественности пользователей облака и распределение ответственности за информационную безопасность между организацией-собственником облачной платформы, интернет-провайдером и организацией-пользователем. А любая распределенная ответственность означает ее размывание, а значит появление слепых пятен и зон информационной опасности. Кроме того, экономия достигается за счет резкого снижения уровня компьютерной квалификации для персонала организаций-пользователей облачных плат-

форм. Редко в какой из таких организаций имеются специальные офицеры по информационной безопасности и соответственно системы защиты от разнообразных киберугроз.

Нельзя не выделить как отдельный, сильнодействующий фактор угрозы, кластерный характер происходящей на наших глазах технологической революции. Информационные технологии с коммуницированием как по закрытым, так и по общедоступным сетям, де-факто стали обязательным компонентом таких решающих для мировой экономики направлений, как робототехника, 3D печать, биотехнологии. Со стремительным удешевлением этих технологий, их все расширяющемся распространением, превращением в основу постиндустриальной промышленной революции, интернет становится буквально вездесущим в производственной и экономической жизни.

Особые риски создает теснейшая интеграция информационных и биотехнологий. Удешевление за последние пять лет примерно в семь раз оборудования для сложных биотехнологических процессов, включая генную, иммунную инженерию и т. п., вместе с широко распространившейся практикой коллективного распределенного использования этого оборудования, делает самые сложные биопроизводства и биоконструирование доступным не только для крупных корпораций, но и для самых маленьких компаний, неформальных групп и отдельных лиц. Такая ситуация не только удешевляет и расширяет сферу применения биотехнологий, но и

открывает невиданные ранее возможности для создания кибербиооружия и использования его не только государственными структурами, но и различного рода террористическими группами, а также маньяками-одиночками.

1.5. Великий уравнитель

Кибервойны впервые за долгий период истории дают весомые шансы более слабым, менее технологически развитым государствам и наднациональным силам одержать победу в жестком противоборстве с гораздо более могущественными странами, обладающими превосходящим военным, политическим, экономическим и научно-техническим потенциалом.

Произвести или приобрести высокоуровневое кибероружие могут сегодня не только достаточно ограниченные в ресурсах государства, но и отдельные группы, сети и т. п.

Роль кибероружия, как великого уравнителя сопряжена стремя главными факторами:

• во-первых, кибернетические войны имеют ярко выраженный ассиметричный характер. Страны, обладающие значительным наукоемким сектором экономики, высокотехнологичной производственной сферой и/ или характеризующиеся высоким уровнем внедрения интернета в повседневную жизнь социума, гораздо более уязвимы для применения кибероружия. Когда интернет является одной из несущих конструкций всей инфраструктуры, высокий уровень его защиты становится на практике почти невозможным. Например, подсчитано, что для того, чтобы на должном уровне обеспечить информационную безопасность только военных,

правительственных и критических корпоративных и общесоциальных электронных сетей и объектов в США, необходимо потратить сумму средств, неподъемную для американской экономики. В эквиваленте она превышает долю фактических расходов на оборону в государственном бюджете, которые был вынужден нести Советский Союз, чтобы выдержать гонку вооружений, и которая в значительной степени подорвала его экономику;

• во-вторых, в современном мире действует принцип коммулятивности рисков. Страны и их военно-политические объединения несут тем большие риски применения против них кибероружия, чем в большем числе военных конфликтов высокой и низкой интенсивности, гражданских войн и острых внутриполитических противоборств в третьих странах они участвуют. Более того, высокая инерционность социума приводит к тому, что аккумулирование рисков происходит в течение длительного периода времени и активное участие в том или ином конфликте может иметь последствия в виде применения кибероружия через несколько лет, а то и десятилетий после его завершения;

• в-третьих, специалистам по системотехнике и теории сложности, вовлеченным в разработку военной политики хорошо известен такой термин, как «ловушка сложности». Очевидно, что синхронное развитие технологий, формирующих следующий технологический уклад, неизбежно ведет не только к росту могущества во всех его компонентах, но

и делает страну гораздо более уязвимой для кибератак. Чем шире применяются во всех сферах жизни информационные технологии, чем сложнее электронная инфраструктура, тем ниже ее совокупная надежность. На практике это проявляется в возрастании риска лавины отказов. Она может иметь началом относительно небольшие технические сбои в периферийных секторах информационной инфраструктуры, которые затем распространяются в сети по каскадному принципу. Этот принцип для наглядности часто называется «эффектом домино».

Представляется, что зачастую высокие руководители различных рангов, в отличие от специалистов по информационной безопасности и кибервойнам не вполне отдают себе отчет в роли кибероружия, как великого уравнителя, и практических последствиях действия трех, указанных выше, факторов. Например, в марте 2013 года Глава АНБ и Киберкомандования США Генерал Кейт Александер, отвечая на вопросы в Конгрессе, подчеркнул: «Мы уверены, что наша кибероборона является лучшей в мире».

Приведем лишь несколько примеров, заставляющих усомниться в эффективности американской кибероборонны. Как показывает практика, она не только не позволяет отразить массированные кибератаки, но и не может сдержать проникновение в закрытые сети хакерских групп.

В конце апреля американская пресса сообщила, что в январе 2013 года хакеры сумели получить доступ к Националь-

ному реестру плотин – закрытой базе данных, которую ведет Инженерный корпус армии США. База охватывает данные обо всех 79 тыс. плотин на территории Америки, включая 8,1 тыс. наиболее крупных плотин, регулирующих водопотоки и водоснабжение крупнейших городов, объектов национальной безопасности, центров критической инфраструктуры и т. п. База содержит наряду с прочим результаты обследования по каждой плотине с указанием их слабых, уязвимых мест, а также оценку возможного количества погибших в случае прорыва, повреждения и т. п. Самое поразительное, что проникновение на сервер с информацией произошло в январе, а было обнаружено только в конце апреля.

О высокой уязвимости американских сетей к проникновению говорят сами американцы. Выступая в 2013 году, Глава Комитета по разведке Конгресса США Майкл Роджерс, отметил, что китайским кибершпионам удалось похитить научно-техническую документацию по более чем 20 особо секретным военно-технологическим разработкам. Общие же потери от китайского экономического кибершпионажа, связанные с хищением интеллектуальной собственности, он оценил в сумму порядка 150 млрд, долларов за последнее время.

Другим характерным примером является получение доступа хакерами к суперкомпьютеру в Национальной лаборатории имени Лоуренса в Бёркли, одному из самых мощных суперкомпьютеров в списке Топ-500. Помимо прочего

этот суперкомпьютер входит в закрытую суперкомпьютерную сеть Министерства энергетики США. Но и это еще не все. Согласно появившимся в последнее время публикациям, суперкомпьютеры Агентства Национальной Безопасности и Министерства энергетики увязаны в единую общеамериканскую сеть суперкомпьютеров, которая используются для нужд обоих ведомств. Самым интересным в этой истории является даже не то, что хакерам удалось подключиться к одному из самых мощных компьютеров в мире, а соответственно и сети суперкомпьютеров, а то, что взлом не был обнаружен техническими средствами. Двадцатичетырехлетний американский хакер Э. Миллер был арестован в результате дачи показаний другим хакером, пошедшим на сделку со следствием. Причем, арестован при попытке продать аренду на доступ к суперкомпьютеру.

1.6. Неопознанная война: эскалация

Кибервойна, в силу трудностей определения инициаторов и инструментария кибератак, времени развертывания кибервооружений и фактического начала боевых действий в киберпространстве, замаскированности во многих случаях ущерба от кибернападений под технические отказы и человеческие ошибки, а также в силу других факторов, без преувеличения может быть названа «неопознанной» войной.

Отдавая себе отчет в принципиально новом характере кибервойн по сравнению с другими видами вооруженных конфликтов, оценивая возможности и угрозы, связанные с этим видом вооружений, американская элита в условиях несомненного лидерства США в сфере информационных технологий приняла несколько лет назад решение о фактическом начале крупномасштабного превентивного кибершпионажа, как первой фазы неопознанной кибервойны.

В марте 2013 года опубликован очередной сводный доклад о глобальных угрозах национальной безопасности США, подготовленный при участии всех 16 разведывательных и контрразведывательных структур США-Statement for the Record Worldwide Threat Assessment of the US Intelligence Community.

В докладе впервые киберугрозы четко и безоговорочно поставлены на первое место и особо выделены из спектра

прочих угроз национальной безопасности США. Причем, киберугрозы в докладе трактуются весьма расширительно. Они включают наряду с атаками на государственные и военные сети, на критически важные объекты и сети, также кибершпионаж, не только в отношении правительственных учреждений, но и американских корпораций. В их состав включаются также хакерские атаки, например, на банки Wall Street и крупнейшие компании электронной коммерции типа Amazon и eBay и т. п. При этом в числе стран, с которыми связываются указанные угрозы, выделяются в первую очередь Китай и Россия.

Впервые в доклад добавлен раздел про угрозу усиления глобального контроля над интернетом со стороны национальных государств и попытку перекраивания глобальной модели управления Сетью, предпринятую Россией, Китаем и Ираном на Всемирной конференции по международной электросвязи (ВКМЭ), проведенной Международным союзом электросвязи в Дубае в декабре 2012 г.

Бывший на тот момент главой АНБ и Киберкомандования США генерал Кейт Александер в марте 2013 года, отвечая на вопросы конгрессменов, особо подчеркнул, что американская доктрина «кибернаступления требует глубокого, постоянного и повсеместного присутствия в сетях противников, чтобы в нужный момент добиться максимального эффекта… Непревзойденный эффект по поражению систем противника будет достигнут за счет американского технологи-

ческого и эксплуатационного превосходства» в сфере информационных технологий. Действующая в настоящее время Президентская Директива № 20, выданная руководителям национальной безопасности и разведки в октябре 2012 года, включает ряд процедур для обеспечения законности кибератак. Директива указывает, что правительство считает, что кибератаки, известные как «Наступательные кибероперации» (OCEO от англ. Offensive Cyber Effects Operations), происходят все чаще и кибернетическая война может быть очень близко.

Наступательные кибероперации могут предоставить уникальные и нетривиальные возможности улучшения позиций США во всем мире «без или с малым предупреждением» противника или цели, с потенциальным воздействием от незначительных до серьезных повреждений», – говорится в Директиве № 20. «Правительство США должно определить потенциальные цели национального значения, где OCEO-операции могут предоставить лучший по сравнению с другими силовыми инструментами государства баланс эффективности и потенциального риска».

Еще в 2008 г. журнал Вооруженных сил США AFJ опубликовал большую статью полковника Чарльза Уильямсона III «Ковровые бомбардировки в киберпространстве». В этой статье полковник Уильямсон пишет: «Америке необходима сеть боевых программ, которые могут направить такое количество трафика на сервера противника, что они больше не

смогут функционировать и превратятся в бесполезные куски металла и пластика. Америка нуждается в создании программ, обеспечивающих эффект ковровых бомбардировок киберпространства. Это позволит получить сдерживающий фактор, которого у нас пока нет». Развивая подход «ковровых бомбардировок в киберпространстве», Президентская директива № 20 предусматривает, что новые наступательные кибероперации «обеспечат потенциальные эффекты, начиная от едва заметного до причиняющего серьезный ущерб». К числу наступательных кибероперациий в Директиве отнесены «перехват управления, нарушение функционирования, физическое уничтожение хранимой информации, компьютеров и их сетей, систем связи, а также управляемых компьютерами объектов физической или виртуальной инфраструктуры». В Директиве предусматривается, что при проведении кибероперациий возможны «очень значительные последствия и разрушения для противника».

Основополагающей информацией, которая с уверенностью позволяет говорить о развертывании Соединенными Штатами сети глобального кибершпионажа, как первой фазы превентивной неопознанной кибервойны, являются сведения о многофункциональных программных продуктах для этих целей.

В 2013 году «Лаборатория Касперского» провела анализ платформы Flame, разработанной ориентировочно в конце 2010 г. и используемой как одна из базисных платформ

для создания кибервооружений. Согласно мнению ведущего эксперта «Лаборатории Касперского» Александра Гостева: «Flame – это троянская программа, бэкдор, имеющая также черты, свойственные червям и позволяющие ей распространяться по локальной сети и через съемные носители при получении соответствующего приказа от ее хозяина. По размеру Flame почти в 20 раз больше Stuxnet и включает в себя много различных функций для проведения атак и кибершпионажа. У Flame нет большого сходства с Stuxnet/Duqu.

Flame-это большой набор инструментов, состоящий более чем из 20 модулей. Назначение большинства связано с тестированием уязвимостей, обеспечением проникновения и его маскировкой, поддержанием долговременного доступа в закрытую сеть через уязвимости, снятием разнообразных типов информации и кражей файлов из сети или аппаратного средства, и, наконец, с разрушением и/или перехватом управления физическими объектами и сетями.

По наблюдениям экспертов в сфере кибербезопасности, хозяева Flame искусственно поддерживают количество зараженных систем на некоем постоянном уровне. Это можно сравнить с последовательной обработкой полей: они заражают несколько десятков, затем проводят анализ данных, взятых на компьютерах жертв, деинсталируют Flame из систем, которые им неинтересны, и оставляют в наиболее важных, после чего начинают новую серию заражений».

Благодаря опубликованному в газете Washington Post от

30.08.2013 г. очередному материалу, основывающемуся на разоблачениях Э. Сноудена, стало известно о наличии обширной программы под кодовым названием GENIE. В рамках этой программы американские компьютерные специалисты осуществляют проникновение в зарубежные сети с тем, чтобы поставить их под негласный контроль США. В бюджетных документах указано, что 652 млн. долларов было потрачено на разработку и использование «секретных имплантатов» (сложных многофункциональных вредоносных программ), при помощи которых ежегодно инфицируются десятки тысяч компьютеров, серверов, маршрутизаторов и т. п. по всему миру.

К концу 2013 года в рамках программы GENIE по всему миру было заражено как минимум 85 тыс. стратегических серверов. Это практически четырехкратное увеличение по сравнению с соответствующим показателем в 2008 г.

Единственным ограничением для АНБ в количестве взятых под контроль аппаратных средств является необходимость использования на сегодняшний день людей-операторов для извлечения информации и осуществления удаленного контроля над взломанными машинами. Даже со штатом 1870 человек GENIE максимально использует только 8448 из 68975 машин с внедренными имплантатами по состоянию на 2011 г. Сейчас АНБ внедряет автоматизированную систему под кодовым названием TURBINE, которая должна позволить в автоматизированном режиме управлять мил-

лионами имплантатов для сбора разведывательной информации и осуществления активных атак, вплоть до разрушения и/или перехвата управления над материальными объектами и сетями по всему миру. На расчетную мощность система TURBINE выйдет с началом полноценной эксплуатации сданного в 2013 г. нового огромного датацентра АНБ в штате Юта.

Согласно опубликованным в составе досье Сноудена документам, программное обеспечение для наступательных операций нацелено, прежде всего, не на отдельные компьютеры, а на сети. Оно решает задачу проникновения в сети противника, используя известные и обнаруживаемые самим Агентством уязвимости, которые содержатся не только в программах и технических средствах, разработанных противником, но и в харде и софте, используемых по всему миру известных брендов, большинство из которых производится в США. В настоящее время по разным оценкам от 65 до 75 % коммерчески реализуемого на мировых рынках программного обеспечения, производится компаниями под американской юрисдикцией. На корпорации из Соединенных Штатов и их ближайших союзников приходится более 85 % производства своего рода «сердца компьютеров» – от планшетников до серверов – процессоров. Как стало известно, подавляющее большинство этих компаний в рамках сотрудничества с американским разведывательным сообществом намерено оставляют в своей продукции те или иные уязвимости, об-

легчающие несанкционированное проникновение и закладку логических бомб, выводящих в нужный момент компьютеры из строя.

В бюджетных материалах, обнародованных Эдвардом Сноуденом, говорится о 231 наступательной кибероперации. Однако из сопроводительных документов к бюджету становится ясным, что это лишь верхушка айсберга. Из анализа опубликованных документов становится понятным, что это активные операции Киберкомандования, санкционированные в соответствии с законодательством высшим руководством Соединенных Штатов. В то же время, в соответствии с законодательством для собственно разведывательных операций в большинстве случаев таких санкций не требуется. Между тем, как видно из анализа компьютерных вооружений, одна и та же программная платформа может использоваться как для кибершпионажа, так и для разрушительных кибероперациий. В отличие от материального мира, чтобы перейти грань между шпионажем и войной в киберпространстве, достаточно только активировать один дополнительный модуль программы, а именно боевую программу на уничтожение или перехват управления материальными объектами и сетями.

Подлинным откровением опубликованных в рамках бюджетного доклада документов из досье Э. Сноудена стала активная вовлеченность ЦРУ в наступательные кибероперации. В чем чрезвычайная важность именно этого факта? Она

состоит в том, что в отличие от АНБ, ЦРУ имеет право вербовать агентов, а также использовать в качестве агентов сторонние, никак не связанные контрактными отношениями с правительством США, компании и организации. В сочетании с информацией о том, что АНБ в 2013 г. потратило более чем 25 млн. долларов на «дополнительные тайные покупки программ обнаружения уязвимостей в программном обеспечении» у частных производителей хакерского софта на так называемом «сером» рынке, это означает возможность для американского разведывательного сообщества вести частные, формально не связанные с правительством США, кибервойны против любой страны мира.

Эти войны могут вестись тайными компаниями-агентами ЦРУ с использованием финансируемого правительством США, но формально никак с ним не связанного, боевого софта. Т. е. фактически кибервойны сколь угодно высокой степени интенсивности против любого противника могут вестись частными кибервоенными компаниями вне всякой формальной привязки к США, но при финансировании и всех видах поддержки со стороны Пентагона и американского разведывательного сообщества. Это означает полную бесконтрольность кибервойн. Особая же опасность состоит в том, что эти квазичастные киберармии могут использовать для своих боевых действий уязвимости, обнаруженные государственным разведывательным софтом в рамках вполне законной деятельности.

Совокупность фактов и сведений позволяет с уверенностью утверждать, что кибервойна США против остального мира, и в первую очередь Китая, России и Ирана уже началась. Пока она находится на первой стадии эскалации, а именно в фазе тотального шпионажа, обнаружения множественных уязвимостей и внедрения в них программ-имплантатов многоцелевого применения. Причем, в любой момент начальная фаза неопознанной войны может по сигналу оператора быть переведена в фазу разрушительных в прямом физическом смысле этого слова военных действий.

Нельзя не отметить, что в первую фазу эскалации кибервойн вступили не одни Соединенные Штаты. Другим крупнейшим актором кибершпионажа, а соответственно и разработки многоцелевых вредоносных разведывательных и боевых программ, является Китай.

По оценкам экспертов в сфере информационной безопасности и кибервойн на сегодняшний день лучшие в мире кибервойска имеются в составе Народно-освободительной армии Китая (НОАК). Китайская армия, технически проигрывая американцам в обычном и ядерном вооружениях, уже долгие годы целенаправленно вкладывает деньги именно в информационные технологии. В итоге ей удалось создать на сегодняшний день наиболее эшелонированную и мощную кибероборону страны, одновременно развивая наступательные кибервооружения. Китай сделал ключевым элементом своей военной стратегии «ассиметричное сдерживание» за

счет создания киберподразделений.

Развитие китайских кибервойск осуществляется в соответствии с пятнадцатилетней стратегией (2006–2020 гг.) информатизации Китая, включающей вопросы использования киберсредств в целях национальной безопасности. Согласно специальному докладу ASPI (Австралийского института стратегической политики, связанного с австралийским разведывательным сообществом) «Enter the Cyber Dragon», опубликованном в июне 2013 г., структура кибервойск Китая выглядит следующим образом.

Китайские кибервойска сосредоточены во Втором, Третьем и Четвертом департаментах НОАК. Причем, решающую роль в кибервойнах призваны играть Третий департамент, обеспечивающий кибершпионаж и киберконтрразведку и Четвертый департамент, ответственный за атаки на компьютерные сети.

Помимо государственных кибервойск, соответствующие подразделения НОАК тесно взаимодействуют с Red Hacker Alliance. RHA является своего рода неформальной, но управляемой государством сетью хакеров, включающую десятки тысяч хакеров из Китая и других стран, в основном из китайской диаспоры по всему миру.

Помимо всемирно известных успехов китайцев в кибершпионаже, уже зафиксировано несколько случаев использования ими сложных платформ, типа многофункциональных троянов. В частности, они использовались в сентябре

2010 г. против австралийских правительственных сетей, в январе 2012 г. против европейского военного авиакосмического агентства и известной компании по безопасности ASC. Кроме того, многие эксперты связывают с RHA размещение вредоносных имплантатов в сентябре 2012 г. в сетях аэрокосмических предприятий, принадлежащих правительству Индии, а также в марте 2011 г. в сетях RSA – крупнейшей компании-производителе электронных ключей безопасности. В результате, предположительно, китайским хакерам удалось проникнуть в корпоративные сети крупнейших подрядчиков Пентагона L-3 Communications Lockheed Martin и Northrop Groumman, и изъять стратегически важную научно-техническую и технологическую документацию, касающуюся военных разработок.

Наряду с Соединенными Штатами и Китаем объявили о создании киберподразделений в составе вооруженных сил Израиль, Великобритания, Иран, Германия и т. п.

1.7. На пути к кибермиру

Несмотря на развернувшуюся гонку кибервооружений и фактически начало пассивной фазы кибервойны, в долгосрочной перспективе, новая цифровая война не соответствует интересам ни одной из стран мира и может иметь трудно-предсказуемые экономические, политические, а возможно и военные последствия для всех. Поэтому крупномасштабной кибервойны необходимо избежать.

Необходим кибермир, который базируется на цифровом равенстве и равном доступе, правах и ответственности всех суверенных государств в отношении всемирной Сети. Именно эти принципы заложены в «Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г.» Сходных позиций придерживаются и другие участники таких организаций, как БРИКС, ШОС, ЕврАзЭС.

Предотвратить переход из пассивной в активную фазу кибервойны могут только согласованные усилия мирового сообщества, и в первую очередь тесное сотрудничество и взаимодействие стран-лидеров в сфере информационных технологий в целом и информационной безопасности, в частности.

Первым необходимым шагом на этом пути, предусмотренным «Основами государственной политики Российской

Федерации в области международной информационной безопасности на период до 2020 г.» является интернационализация управления интернетом под эгидой ООН, обеспечение цифрового равенства и суверенитета всех стран.

Переход от сегодняшнего и де-факто, и де-юре нерегулируемого в международном масштабе интернета к ясной и понятной схеме единого интернета, состоящего из информационных пространств суверенных стран, позволит четко определить не только права, но и ответственность каждой страны за соблюдение безопасности интернета в целом и отдельных его сегментов. На практике это означает, что страна должна нести ответственность за акты киберагрессий, которые осуществляются из или с использованием информационного пространства страны. Естественно, что мера ответственности должна зависеть от степени вовлеченности страны в провоцирование или участие в кибервойне. При этом в соответствующих международных соглашениях, по мнению экспертов, должны быть четко прописаны возможные санкции и условия их применения к стране-нарушителю. В условиях, когда агрессором могут быть не только государственные или частные структуры, но и неформализованные сетевые образования, признание цифрового суверенитета означает государственную ответственность за пресечение деятельности таких организаций и образований, прежде всего, силовыми структурами самой страны, а при необходимости и с согласия страны – с подключением международной помощи.

Изменение структуры управления Интернетом и разработка соответствующих международных соглашений естественно потребуют определенного времени, но все потенциальные участники этого процесса должны понимать, что распространение кибервооружений происходит не по годам, а буквально по месяцам. Соответственно возрастают риски кибервойны и кибертерроризма. Поэтому в данном случае необходима быстрая и согласованная работа всех заинтересованных государств.

Другой очевидной и возможно непопулярной мерой по пресечению неконтролируемого распространения кибервооружений и их частной разработки является ужесточение контроля не только за интернетом, но и другими альтернативными интернету сетями, включая так называемые мэш- и пиринговые сети. Причем, речь идет не только о деанонимизации интернета и пользователей электронных коммуникаций в широком смысле этого слова, но и о расширении предусмотренного национальными законодательствами возможностей государственного контроля за деятельностью компаний и отдельных лиц, задействованных в разработках в сфере информационной безопасности, а также отработке методик тестирования проникновения. Многие полагают, что одновременно должны быть ужесточены национальные законодательства в части хакерской деятельности, наемничества в сфере информационных технологий и т. п.

В современном мире выбор между ничем не ограничен-

ной личной свободой и ответственным, укладывающимся в социально безопасные рамки поведением, перестают быть темой для дискуссий и предметом для спекуляций. Если национальные правительства и международное сообщество хотят предотвратить кибервойны, то необходимо публично и открыто ввести соответствующие нормы в национальные и международное законодательства. Эти нормы должны позволить усилить суверенный технический контроль над поведением, частной и коммерческой деятельностью в интернете с целью обеспечения национальной и международной безопасности в киберпространстве.

Возможно, заслуживает также обсуждения вопрос о создании на базе потенциала ведущих в сфере информационных технологий стран, прежде всего, Соединенных Штатов, России, Китая, Великобритании, Японии и др. международных сил по раннему обнаружению и пресечению угрозы кибервойн. Создание таких международных сил позволило бы с одной стороны в ускоренном порядке мобилизовать в значительной степени взаимодополняющий потенциал различных стран для пресечения кибервойн, а с другой стороны волей-неволей сделало бы их разработки более открытыми, а соответственно и менее угрожающими для других участников пула, добровольно взявших на себя повышенную ответственность за соблюдение кибермира.

1.8. Борясь за кибермир, готовься к новым кибервойнам

При всем стремлении к миру, как показывает российская история, безопасность страны может быть обеспечена только при наличии мощных оборонительных и наступательных кибервооружений.

Согласно сообщениям российских информационных агентств, в российской армии в текущем году сформированы и приступили к выполнению своих задач специальные подразделения, которые занимаются борьбой с киберугрозами. Эти подразделения способны не только отражать кибератаки на нашу страну, но и при необходимости вести наступательные кибероперации. В их состав по информации заместителя министра обороны РФ Павла Попова входит в том числе структура, осуществляющая глубинный анализ хакерского программного обеспечения и декодирование любых телекоммуникационных протоколов.

Чтобы успешно решить задачу форсированного создания кибервойск, у России есть все необходимые предпосылки. Следует помнить, что в отличие от многих других отраслей, российские компании, занимающиеся информационной безопасностью и тестированием уязвимостей, входят в число мировых лидеров и продают свою продукцию на всех континентах. Русские хакеры стали всемирно известным брендом.

Подавляющая часть софта, обслуживающего высокочастотный трейдинг и наиболее сложные финансовые операции на всех основных биржевых площадках мира, созданы российскими программистами и разработчиками. Такие примеры можно множить и множить. И относятся они, прежде всего, к созданию софта, требующего высочайшего уровня математической подготовки и знания наиболее сложных языков программирования.

В отличие от многих других направлений науки и техники в России, научные школы по математике, компьютерным наукам и программированию, за последние 20 лет не только не потерпели урона, но и значительно развились, вышли на лидирующие мировые позиции. Такие российские ВУЗы, как МФТИ (ГУ), МГУ им. Ломоносова, МГТУ им. Баумана, НИЯУ МИФИ, Санкт-Петербургский государственный университет, Ульяновский государственный технический университет, Казанский государственный университет и т. п. являются признанными центрами подготовки ал го ритм и сто в, разработчиков и программистов мирового уровня. Из года в год российские команды программистов выигрывают мировые первенства по программированию среди университетов. Работы отечественных алгоритмистов постоянно цитируются в ведущих мировых журналах. Российские математики постоянно входят в число соискателей премии Филдса.

Кстати, интересно, что в разгар скандала со Сноуденом, одна из ведущих американских организаций по изучению

общественного мнения Pew Internet & American Life Project провела опрос, кто в наибольшей степени угрожает конфиденциальности личной и корпоративной информации. Итоги оказались таковы. 4 % – силовые структуры, 5 % – правительства, 11 % – другие бизнес-структуры, 28 % – рекламодатели и интернет-гиганты и 33 % – хакеры. При этом, по мнению едва ли не самого популярного издания об интернет-технологиях в Америке, журнала Wired, несомненную пальму первенства среди хакеров держат русские хакеры.

Иными словами, необходимый научный, технологический, программный и кадровый задел для ускоренного формирования грозных кибервойск в России имеется. Вопрос состоит в том, каким образом привлечь в кибервойска, а также компании, которые будут включены в программу национальной кибербезопасности, наиболее квалифицированных, талантливых разработчиков, программистов, тестировщиков систем информационной безопасности и т. п. Здесь важно не повторить ситуацию, которая имеет место сегодня в отраслях военно-промышленного комплекса, где из-за низких зарплат качественные кадры не задерживаются и уходят в различного рода коммерческие разработки, зачастую имеющие иностранных инвесторов.

В мире сложилось три основных направления рекрутирования лучших программистских кадров в государственные программы, связанные с кибервойнами. Наиболее известен опыт Соединенных Штатов. Он базируется на своего рода

трех китах. Во-первых, ежегодно DARPA проводит множество конкурсов, мероприятий, круглых столов для программистского сообщества, где идет отбор наиболее талантливых, подходящих для задач Пентагона и разведки, молодых людей. Во-вторых, практически все ведущие IT компании Соединенных Штатов связаны с военно-разведывательным сообществом и программисты соответствующих подразделений частных компаний, многие из которых даже не являются подрядчиками Пентагона в своей повседневной деятельности, заняты разработкой программ в сфере кибервооружения. В-третьих, АНБ непосредственно взаимодействует с ведущими американскими университетами, а также в обязательном порядке присутствует на всех общенациональных хакерских конференциях и черпает кадры оттуда.

Китайский подход базируется на строгой государственной дисциплине и руководящей роли КПК в решении ключевых кадровых вопросов китайских вооруженных сил. По сути, для китайского программиста или разработчика работа над кибервооружениями является проявлением долга, ключевой характеристики поведенческих паттернов китайской цивилизационной традиции.

Что же касается Европы, то здесь сделан упор на поддержку в большинстве стран ЕС движения так называемых «этичных хакеров», т. е. разработчиков и программистов, которые не занимаются противоправными действиями, а специализируются на сотрудничестве с коммерческим сектором в ча-

сти обнаружения информационных уязвимостей и силовыми структурами, в части создания кибервооружений.

Представляется, что в России можно в той или иной мере использовать элементы и американского, и европейского, и китайского опыта. При этом вполне очевидно, что главным должно стать понимание со стороны государства, что в сфере цифровых войн именно человеческий фактор является определяющим при разработке и использовании оборонительных и наступательных кибервооружений.

В этой связи всячески следует развивать инициативу создания научных рот, прямую государственную поддержку стартапов, связанных с разработкой программ в сфере информационной безопасности, тестирования проникновений и т. п. Необходимо, конечно же, провести тщательную инвентаризацию имеющихся уже сегодня в России разработок, которые при определенном апгрейде могли бы стать мощными кибервооружениями. Такая инвентаризация необходима потому, что в силу серьезных недостатков и коррупции при проведении государственных тендеров, подавляющее большинство маленьких компаний и талантливых программистов, по сути, отсечено от этой задачи и не востребовано силовыми структурами.

Понятно, что государству, как это не парадоксально, надо повернуться лицом к хакерам.

Наряду с возможным ужесточением уголовных наказаний за компьютерные преступления, государство должно предо-

ставить возможность хакерам применить свои способности и навыки в общественно-полезной деятельности и, прежде всего, в разработке кибероборонительных и кибернаступательных вооружений, тестировании сетей на предмет злонамеренного проникновения. Возможно, заслуживает обсуждения идея о создании своего рода «хакерских штрафбатов», где разработчики, программисты и тестировщики, имевшие те или иные правонарушения в России или за рубежом, могли бы делом искупить свою вину.

И, конечно же, следует помнить, что едва ли не самые востребованные профессии в мире на сегодняшний день – это разработчики, программисты, специалисты по Большим Данным и т. п. Их зарплаты стремительно растут и в нашей стране и за рубежом. По независимым оценкам американских и российских экспертов, до 20 тыс. российских программистов сейчас трудятся в США. Поэтому, памятуя, что в кибервойсках ключевое звено – это разработчик, программист, патриотичный хакер, на их оплату и социальный пакет не надо жалеть денег, также как не экономили в свое время деньги на зарплату и бытовые условиях ученых и инженеров при разработке советского атомного проекта.

Оборонительные и наступательные кибервооружения являются одной из немногих сфер, где Россия высококонкурентна на мировой арене и может в короткие сроки создать программные средства, способные не только заметно повысить уровень безопасности собственных критически важных

сетей и объектов, но и за счет наступательных возможностей сдержать любого потенциального киберагрессора.

Кибероружие для России – это реальный и серьезный шанс ассиметричного ответа на гонку высокоточных вооружений, развязанную в мире и один из ключевых элементов достаточной национальной безопасности.

1.9. Кибероружие сдерживания

На сегодняшнем уровне развития информационных технологий, включая средства киберзащиты и цифрового нападения, такие страны как Россия и Китай могут успешно противодействовать планам развязывания крупномасштабной активной кибервойны со стороны таких потенциальных агрессоров, как США и их союзники, в первую очередь Великобритания, Франция, Израиль.

Правящая элита США отдает отчет в сегодняшней уязвимости своей страны перед угрозой сколько-нибудь масштабной цифровой войны. Пожалуй, это является главным фактором, сдерживающим переход пассивной фазы цифровой войны в активную, связанную с применением наступательных, разрушительных кибервооружений.

В этих условиях часть американской элиты делает ставку на конвертацию сложившегося превосходства Соединенных Штатов в сфере информационных и других технологий седьмого технологического уклада в создание кибервооружений нового поколения.

Эти кибервооружения и решения в сфере информационной безопасности США призваны преодолеть нынешний ассиметричный характер кибервойн и сделать страны – потенциальных противников США беззащитными перед американской кибермощью.

Вопросы новейших разработок в сфере кибервооружений являются, естественно, тайной за семью печатями американского военно-промышленного комплекса. Однако внимательный анализ тенденций развития информационных технологий и опубликованных в СМИ государственных документов США позволяют сделать ряд выводов о мерах, предпринимаемых по достижению неоспоримого кибердоминирования.

Еще в 70-90-е годы прошлого века в ходе исследований, направленных на создание искусственного интеллекта, проводимых в СССР, США и Японии, была создана математическая база и алгоритмическая основа для так называемых самосовершенствующихся программ, заложены основы генетического и эволюционного программирования. Была создана математико-алгоритмическая база для разработки программ, которые могли бы самообучаться в зависимости от поступающих из внешней среды сигналов и соответственно трансформироваться в сторону все более эффективного выполнения своих функций. Позднее одно из ответвлений этого направления получило название «машинное обучение». В прошлом веке для практической программной реализации этого подхода не было аппаратных возможностей. Что называется, не хватало вычислительных мощностей.

В середине прошлого десятилетия критический порог был перейден, и машинное обучение, как основа для решения широкого круга задач, стало активно развиваться и

реализовываться на базе суперкомпьютеров. Наиболее известной демонстрацией возможностей машинного обучения и эволюционного программирования стал знаменитый Watson. В 2011 г. суперкомпьютер IBM победил экспертов, чемпионов американской версии «Своя игра». В настоящее время Watson активно используется для диагностических и прогнозных целей в здравоохранении, страховании и сфере национальной безопасности США.

Некоторые эксперты полагают, что огромные сети имплантатов, выполняющие шпионские функции, будучи подсоединенными к подобной экспертной системе и способные к машинному обучению, могут стать боевыми самообучающимися киберпрограммами. Образно говоря, передавая информацию в экспертную систему, они получают от нее команды, позволяющие этим программам, как бы самим достраиваться, адаптируясь к конкретным параметрам зараженных компьютеров и сетей. По мнению специалистов, скорее всего такие программы будут применяться не столько для разрушения, сколько для незаметного перехвата управления критически важными объектами и сетями потенциального противника.

Чтобы от машинообучаемых перейти к полноценным самоизменяющимся и самоорганизующимся программам, необходимо задействовать даже не сегодняшние суперкомпьютеры, а суперкомпьютеры следующего поколения с еще большей степенью быстродействия. В этом случае однажды

разработанная многомодульная программа-имплантат, в зависимости от конкретных условий и стоящих задач, сможет достраивать свои модули, адаптироваться и предупреждать действия по ее обнаружению или уничтожению. Более того, недавно в специальных научных журналах а также в Wall Street Journal была опубликована информация о том, что такие самоорганизующиеся программы-имплантаты смогут выводить из строя объекты никак не подключенные к интернету, а функционирующие в закрытых сетях. Причем, в этих публикациях утверждается, что найден способ проникновения программ-имплантатов этого класса даже в отключенные сложные компьютеризованные объекты, линии, энергосистемы и т. п. При переходе этих объектов в активный режим программы реализуют свои задачи разрушения, либо перехвата управления. Эти программы и имплантаты для проникновения используют акустическую и оптическую среды.

На сегодняшний день самым мощным суперкомпьютером в мире является китайский Тяньэх-2. Большая часть компонентов этой системы была разработана в Китае. Однако надо иметь в виду, что подавляющая часть наиболее мощных суперкомпьютеров принадлежит Соединенным Штатам и в отличие от Китая, соединена в единую распределенную сеть под эгидой АНБ и Министерства энергетики США. Но главное даже не это. Чтобы осуществить следующий скачок в скорости вычислений, необходимо переходить уже на

уровень нанотехнологий. Летом этого года ведущие американские производители процессоров для суперкомпьютеров объявили о том, что к 2015 г. они смогут начать производство микропроцессоров, пока еще на основе кремния, но уже со значительным использованием нанотехнологий. Приближаются к подобному решению и японцы.

Китай, наращивая мощность суперкомпьютеров, пока, судя по оценкам экспертов, не имеет необходимой технологической базы для производства процессоров с использованием нанотехнологий. Ключевым вопросом в обеспечении превентивного доминирования в киберпространстве является способность декодировать защищенную специальными шифрами информацию, передаваемую как в интернете, так и в закрытых сетях государств – потенциальных противников. Согласно документу АНБ, обнародованному Сноуденом, «в будущем сверхдержавы будут появляться и приходить в упадок в зависимости оттого, насколько сильными будут их криптоаналитические программы. Это цена, которую должны заплатить США, чтобы удержать неограниченный доступ к использованию киберпространства».

Уже давно Агентство на постоянной основе работает с IT-компаниями по встраиванию в их продукты закладок в интересах спецслужб США, а также ведет работу по целенаправленному ослаблению международных алгоритмов защиты данных. Поскольку именно американские компании являются поставщиками подавляющей части используемых

в мире процессоров, маршрутизаторов, серверной инфраструктуры и т. п., становится понятным, что на сегодняшний день в подавляющем большинстве стран, в том числе в России, даже закрытые компьютерные сети весьма уязвимы для проникновения, а используемые системы шифрования в значительной части являются прозрачными для американских спецслужб.

Хотя в опубликованных Э. Сноуденом документах и имеется информация, что службы США и Великобритании могут взломать любой шифр, используемый в интернете, это, по мнению подавляющего большинства специалистов, не является корректным утверждением. Более того, тесные контакты АНБ с производителями харда, в который они стремятся встроить соответствующие закладки, лишний раз подтверждает это мнение.

Проблема состоит в том, что мощностей нынешних суперкомпьютеров, даже в виде распределенной сети не хватает для уверенного взлома наиболее изощренных шифров, используемых в правительственной связи и коммуникациях спецслужб информационно продвинутых стран мира, включая Россию.

Однако, ситуация изменится с появлением на свет квантового компьютера. Собственно, одна из сверхзадач квантовых компьютеров как раз и состоит во взломе любого шифра, созданного на традиционных, доквантовых компьютерах. На сегодняшний день математически доказана справедливость

подобной постановки задачи. Против квантового компьютера все доквантовые системы шифрования бессильны.

Хотя самих квантовых компьютеров пока нет, уже созданы многочисленные алгоритмы для них, а буквально в этом году по заданию IARPA разработан язык программирования Quipper. Работы по практическому созданию квантового компьютера ведутся в Соединенных Штатах в рамках проекта Quantum Computer Science (QCS) IARPA.

Немаловажно понимать принципиальное отличие IARPA от DARPA. Помимо прочего оно состоит в том, что проекты DARPA относятся к сфере двойных технологий, предусматривают оповещение о разработчиках тех или иных проектов и их результатах. Вся информация по проектам IARPA, кроме их наименования и условий, является секретной.

В 2013 году совершен прорыв и в аппаратном компоненте квантового компьютера. Компания Google, совместно с NASA запустила в эксплуатацию в рамках сети суперкомпьютеров квантовый модуль D-Wave Two. Это еще не полноценный квантовый компьютер, но при выполнении сложных вычислений с более чем 500 параметрами его мощность в тысячи раз превосходит производительность лучших суперкомпьютеров из списка Топ-500.

По осторожным высказываниям Google в ближайшие два-три года они собираются создать сеть, включающую несколько подобных модулей, работающих вместе с обычными суперкомпьютерами, которые по своим совокупным возмож-

ностям вплотную приблизится или будет равна полноценному квантовому компьютеру.

Когда это произойдет, то помимо прочего, любой шифрованный трафик окажется полностью открытым и свободно читаемым, а саморазвивающиеся программы позволят в этих условиях беспрепятственно ставить под контроль любые объекты и сети потенциальных противников. Тем самым будет достигнуто фактически неограниченное доминирование в киберпространстве. Электронные сети противника в любой момент могут быть разрушены или поставлены под полный контроль кибреагрессора, обладающего описанными выше программными и аппаратными средствами. Тем самым кибервойна закончится, не успев начаться.

Но и это еще не все. Летом 2013 года, несмотря на разоблачения АНБ и американского разведывательного сообщества, в Соединенных Штатах состоялся ряд совещаний по повышению уровня кибернетической национальной безопасности. Впервые за всю историю всерьез обсуждался вопрос создания общеамериканской электронной стены – фаервола. В этом случае весь интернет-трафик, входящий из-за рубежа подвергался бы глубокой инспекции пакетов, и любые подозрительные пакеты блокировались так же, как великий китайский фаервол блокирует нежелательные сайты. Участники обсуждения пришли к точке зрения, что это был бы лучший способ, но решили, что подобный подход будет невозможно реализовать на практике из-за американ-

ских реалий. Однако приведенные в докладе опросов американского общественного мнения и руководителей американских корпораций, а также подогреваемые СМИ истерия по поводу китайских и русских хакеров, могут создать питательную почву для практических шагов в этом направлении.

Согласно анализу, проведенному по открытым источникам экспертами Центра военно-промышленной политики Института США и Канады, американцы взяли курс на развертывание автономных спутниковых группировок, обеспечивающих защищенные электронные коммуникации и развертывание системы ПРО, нацеленной не столько против террористов, сколько против потенциальных американских конкурентов в космосе.

Спутниковые группировки призваны создать параллельную современному интернету защищенную систему электронных коммуникаций, завязанную на выведенную в космос суперкомпьютерную систему с квантовыми составляющими. Другая часть орбитальных спутниковых группировок призвана вывести из строя телекоммуникационные и электронные сети противников, способные функционировать в случае принудительного отключения обычного интернета. Наконец, система ПРО должны блокировать запуски ракет противника, нацеленных на орбитальные группировки и космическую платформу с центральным квантовым или квантовоподобным суперкомпьютером.

В этой связи возникает проблема разработки киберору-

жия сдерживания.

Недавно президент РАН Владимир Фортов сообщил, что «Работы, проведенные под руководством академика Геннадия Месяца, позволили создать генераторы, испускающие очень короткие и мощные импульсы. Их пиковая мощность достигает миллиардов ватт, что сопоставимо с мощностью энергоблока АЭС. Это более чем в 10 раз превышает зарубежные достижения». Указанный генератор может быть размещен на носителе, выведенном в космос на низкую орбиту или в мобильном варианте на земле, либо даже на подводной лодке вблизи берегов потенциального противника. Использование такого генератора позволяет получить направленный мощнейший электромагнитный импульс, способный полностью вывести из строя любую электронику, независимо от ее защиты на весьма значительных площадях. Более того, имеются расчеты, показывающие возможность вывести из строя при помощи системы указанных генераторов энергосистемы, телекоммуникации, электронные сети, включая интернет, в самых разных странах мира, в том числе в США.

Какие выводы можно сделать из вышеприведенного анализа и складывающейся внешнеполитической ситуации?

• Грубейшее вмешательство США и их союзников в украинский кризис, события вокруг Сирии показывают, что у геополитических конкурентов России нет никаких моральных ограничений в реализации любых агрессивных планов и провокаций самого чудовищного типа (с уничтожением мир-

ного населения химоружием для обоснования начала войны против суверенной страны в обход международного права). Поэтому скорейшее полноценное развертывание российских кибервойск в структуре вооруженных сил и разработка кибероружия сдерживания являются в современный период не менее важной государственной задачей, чем поддержание в боевой готовности ядерного потенциала.

• Информационный взрыв, связанный с опубликованием в открытой печати сверхсекретных материалов Сноудена о ведущейся кибервойне армией и спецслужбами США против России и других стран, и применяемых при этом технологиях, ставит задачу внесения серьезных корректив в государственную политику обеспечения кибербезопасности. Речь идет о пересмотре стратегических документов, увеличении бюджетного финансирования, ускоренной и качественной подготовке кадров, способных вести противоборство в киберпространстве.

• Сдерживание кибервойн XXI века невозможно без развития фундаментальных научных исследований самой различной направленности. По всей видимости, процесс реализации фундаментальных научных разработок как и прежде будет ориентирован в первую очередь на военные цели для достижения превосходства над потенциальным противником. Причем скорость реализации фундаментальных открытий в прикладных военных целях в условиях идущей информационной революции будет неизменно возрастать. Поэтому

государственные бюджетные вложения в фундаментальные исследования должны быть качественно увеличены.

Глава 2
Информационные войны 3.0

В отечественной военной традиции широко используется известный афоризм классика военной мысли Карла Клаузевица: «Война есть продолжение государственной политики иными средствами». Между тем, для информационных войн гораздо больше подходит другое его высказывание: «Война – это акт насилия, имеющий целью заставить противника выполнить нашу волю».

В этой связи характерно, что в концептуальном документе Пентагона – «Основополагающей концепции ведения объединенных операций – 2020» (сентябрь 2012 года) указано: «Война остается столкновением между враждующими, независимыми и непримиримыми волями, каждая из которых стремится достичь доминирования над другой посредством насилия. Противники будут продолжать свои стремления найти и использовать уязвимости США. Даже если конфликт будет вестись с использованием самых современных технологий, ведение военных операций остается по большому счету делом человека».

Это совершенно не случайно, поскольку агрессивная информационная составляющая стала неотъемлемым элементом военной доктрины Запада, начиная со времен Первой

мировой войны.

К настоящему времени можно выделить два поколения информационных вооружений. Первое поколение связано с использованием в ходе военных действий или подготовки к ним пропаганды, как вида информационных вооружений. На этом этапе объектом интенсивного информационного воздействия были массы военнослужащих и населения стран-противников. Начало второго этапа датируется 70–80 годами прошлого века. Если на первом этапе в военном деле использовались методы пропаганды и рекламы, то второй этап связан с использованием в качестве вооружений методов и технологий маркетинга. Для информационных войн 2.0 характерны самые разнообразные каналы воздействия на сознание, способы подачи информации, включая комбинирование текстовых, визуальных и звуковых сообщений, переход к интерактивным методам. Главной же чертой является ориентация не на массы, а на четко выделяемые группы военнослужащих и населения стран противника, обладающих определенными характеристиками.

В настоящее время мы являемся свидетелями формирования третьего поколения информационных вооружений, используемых в информационных войнах 3.0. С предыдущими поколениями их роднит нацеленность на перепрограммирование сознания в нужном для агрессора направлении, парализацию и подчинение воли руководителей, военнослужащих и населения стран-противников. Принципиально но-

вым для информационных войн 3.0 является то, что в решающей степени они направлены на разрушение активных групповых субъектов, противодействующих агрессору, и напротив, конструирование новых групповых субъектов, являющихся проводниками интересов и исполнителями воли нападающей стороны внутри вооруженных сил, элиты и социума государства – жертвы агрессии.

2.1. Взлет и падение «мягкой силы»

Дж. Най без сомнения относится к числу наиболее влиятельных представителей американского политического истеблишмента. Его книги издаются и переиздаются на многих языках мира. Его воззрения оказывают прямое и непосредственное влияние на государственную политику США времен президента Б. Обамы.

За рубежом, в том числе и в России Дж. Най относится к числу наиболее известных американских политологов. Соответственно, складывается впечатление, что именно его концепция на сегодняшний день представляет собой последнее слово в американской внешнеполитической мысли. Однако на практике дело обстоит несколько сложнее. Чтобы понять ситуацию, сложившуюся вокруг концепции «мягкой силы», необходимо внимательнее присмотреться к истокам ее формирования.

Дж. Най является не только крупнейшим исследователем и знаменитым профессором, но и был длительные годы практикующим политиком, занимавшим ключевые посты в разведывательном, военном и дипломатическом секторах американского правительства.

Ключевым моментом для формирования подхода Дж. Ная стала его теснейшая связь с Дэвидом Рокфеллером. Перед своей государственной карьерой он был одним из основных

функционеров знаменитой в свое время Трехсторонней комиссии. Трехсторонняя комиссия была организована влиятельнейшей финансово-энергетической группой американской элиты – кланом Рокфеллеров. Главной целью комиссии, созданной в начале 70-х годов, была координация усилий американской, европейской и японской элит в деле построения нового мирового порядка и противодействия СССР. В своих мемуарах Дэвид Рокфеллер писал: «Некоторые даже верят в то, что мы (семья Рокфеллеров) являемся частью секретной политической группы, работающей против жизненных интересов Соединённых Штатов, и характеризуют мою семью и меня как «интернационалистов», вступивших в сговор с другими группами по всему миру для построения более интегрированной глобальной политической и экономической структуры-единого мира, если угодно. Если обвинение заключается в этом, то я признаю себя виновным, и я этим горжусь».

Собственно Трехсторонняя комиссия и стала одним из инструментов формирования тех наднациональных элитных сетей, которые вместе с государствами являются основными акторами сегодняшней мировой политики и экономики.

Трехсторонняя комиссия, по сути, стала рабочим органом глобалистского направления в мировой элите. Работы Дж. Ная в этом смысле представляют собой идеологическое обоснование не национально ориентированной американской внешней политики, а базу для глобальной геополи-

тики, осуществляемой в интересах наднациональных элит высшим государственным аппаратом Соединенных Штатов. Нетрудно заметить, что между национальными интересами государства США и интересами наднациональных элит имеются серьезные различия.

Необходимо отметить, что в американском политическом истеблишменте интересы глобалистов наиболее полно представлены так называемым кланом Клинтонитов. Он помимо собственно семьи Клинтонов включает в себя обширную и разветвленную группу политиков, администраторов, военных, финансистов и т. п., чье выдвижение опять же прямо или косвенно связано все с той же Трехсторонней комиссией. Дж. Най является одним из представителей этого клана.

Впервые концепция «мягкой силы», разработанная в недрах Трехсторонней комиссии была представлена в 1990 году. В книге «Bound to Lead: The Changing Nature of American Power» («Призвание к лидерству: меняющаяся природа американской силы») Дж. Най разделяет мощь государства на две составляющих: так называемую «жесткую силу» (hard power) и «мягкую силу» (soft power). Под «жесткой силой» подразумевается совокупная политическая, экономическая и финансовая мощь, а «мягкая сила» в основном характеризуется культурой, ценностями и политической идеологией.

В книге «Мягкая сила. Средства достижения успеха в мировой политике», вышедшей в свет в 2004 году, понимание «мягкой силы» раскрывается следующим образом: «Ес-

ли Наполеон, распространявший идеи Французской революции, был обязан полагаться на штыки, то ныне, в случае с Америкой, жители Мюнхена, равно как и москвичи, сами стремятся к результатам, достигаемым лидером прогресса». И далее автор подчеркивает: «Когда ты можешь побудить других возжелать того же, чего хочешь сам, тебе дешевле обходятся кнуты и пряники, необходимые, чтобы двинуть людей в нужном направлении. Соблазн всегда эффективнее принуждения, а такие ценности, как демократия, права человека и индивидуальные возможности, глубоко соблазнительны».

На постах директора национальной разведки и заместителя министра обороны Дж. Най пытался на практике реализовывать свою концепцию. Однако по оценке подавляющего большинства политиков, практиков, а также представителей военной и разведывательной элиты, не слишком преуспел в замене «жесткой силы» на «мягкую».

Главные аргументы критиков сводились к следующим. Методы «мягкой силы» включают в себя в первую очередь культурную политику, активные мероприятия по продвижению ценностей и идеалов так называемого свободного мира. Иными словами, идеологии. Однако, как показала вся предыдущая история и подтвердили годы, когда Дж. Най пытался на практике реализовать свою концепцию, применяя «мягкую силу» никогда нельзя планировать временные рамки достижения результата. Весьма условен, если вообще воз-

можен, учет рисков и вероятности успеха подобных мероприятий. И, наконец, практически затруднен объективный анализ – произошли ли перемены в результате осуществления политики «мягкой силы», либо под воздействием каких-либо других факторов.

В этом плане концепция «мягкой силы» гораздо в большей степени обсуждалась в академических кругах и использовалась для ведения информационного противоборства, нежели была принята на вооружение, как базисная концепция реальной внешней политики США.

В итоге Дж. Най сменил государственную службу на преподавательскую работу. Казалось бы, концепция «мягкой силы» уйдет в прошлое вместе с ним. Однако жизнь распорядилась по-иному. Если быть более точным, то не жизнь, а Хиллари Клинтон и группа ее советников.

Готовясь в 2006 году к избирательной кампании 2008 года на пост президента, она инициировала создание в Центре стратегических и международных исследований (ЦСМИ) (Center for Strategic and International Studies, CSIS) комиссии по интеллектуальной власти – «Bipartisan Commission on Smart Power», которую возглавили профессор Дж. Най и Р. Эрмитэдж, бывший высокопоставленный сотрудник администрации Б. Клинтона. Итогом работы комиссии стал доклад «Более умная, более безопасная Америка». В докладе впервые был использован термин «умная власть» (власть интеллекта, smart power). Публично его впервые озвучила

Хиллари Клинтон в своей речи в Сенате непосредственно перед утверждением ее кандидатуры на должность госсекретаря. В своем выступлении она сказала: «Мы должны использовать так называемую «власть интеллекта», полный набор имеющихся у нас средств – дипломатических, экономических, военных, политических, правовых и культурных, – выбирая нужное средство или сочетание средств в каждой конкретной ситуации».

Возникает вопрос, почему столь опытный и эффективный политик, как Хиллари Клинтон для своего дебюта на посту госсекретаря, который достался ей в результате соглашения с группой, которая смогла продвинуть на пост президента мало кому известного Б. Обаму, использовала, казалось бы, скомпрометировавшую себя концепцию.

Как это ни удивительно, данный вопрос не получил своего освещения не в американских, не тем более в российских профессиональных публикациях. В итоге возникает странное впечатление, что возможно наиболее эффективный политик Америки при своем дебюте на посту Госсекретаря говорила совершенно избитые вещи о том, что внешняя политика должна использовать все рычаги воздействия, а культурная политика является одним из важных инструментов внешнеполитической активности. Собственно последний тезис не являлся никакой новинкой и был хорошо известен до «мягкой силы» как минимум с 30-х годов прошлого века. Тем не менее, выбор был далеко не случаен по целому ряду

обстоятельств:

• во-первых, еще в книге 1990 года Дж. Най сделал чрезвычайно важный и принципиальный вывод о «мягкой силе». Он определили ее, как «способность добиваться желаемого на основе добровольного участия союзников, а не с помощью принуждения или выплат. Если Соединённые Штаты замедлят мобилизацию своих ресурсов ради международного лидерства, полиархия может возникнуть достаточно быстро и оказать свое негативное воздействие. Управление взаимозависимостью становится главным побудительным мотивом приложения американских ресурсов, и оно должно быть главным элементом новой стратегии». Х. Клинтон уточнила это следующим образом: «Америка должна научиться делать то, что другие хотят, но не могут. И делать это коллективно». Т. е. впервые в американской внешнеполитической практике глобалистские интересы и глобалистский образ действия вышли на первый план по сравнению с национальными интересами Америки;

• во-вторых, «умная власть» предусматривает использование всего арсенала инструментов, имеющихся в распоряжении Америки и ее союзников, обслуживающих интересы наднациональной мировой элиты. Соответственно, эти инструменты могут и должны использоваться не только поодиночке, но и совместно, подкрепляя друг друга;

• наконец, в-третьих, внимательный анализ доклада, подготовленного Центром стратегических и международных ис-

следований, позволяет прийти к выводу о том, что в качестве союзников, участвующих в глобалистских акциях, рассматриваются отнюдь не только государства. В докладе указано, что на смену пирамиде с жесткой иерархической структурой приходит «паутина разновеликих, разнокачественных и разнообразных действующих лиц, находящихся во взаимодействии». При этом становится понятным, что «в число таких акторов могут включаться не только различные государства, или их образования, но и общественные движения, политические группы, активистские группы внутри стран, на которые направлены действия». В марксистской литературе прошлого века, после гражданской войны в Испании, такие группы называли «пятой колонной».

С учетом отмеченных выше обстоятельств, провозглашенная Х. Клинтон стратегия являлась принципиально новой, поскольку фактически представляла собой механизм использования ресурсов США, других стран, а также групп «пятой колонны» в интересах наднациональной элиты.

На время госсекретарства Х. Клинтон приходится явно неудачное окончательное завершение вывода войск из Ирака, трудности с выводом войск из Афганистана, в целом негативные для Соединенных Штатов события «арабской весны», неуклюжее и бессмысленное вмешательство бывшего посла США М. Макфола во внутренние дела России во время парламентских выборов 2011 года и т. п. Сменивший Х. Клинтон на посту Госсекретаря Дж. Керри также является

выходцем из недр Трехсторонней комиссии. Более того, в период его предвыборной кампании в 2004 году именно Дж. Най рассматривался как основной кандидат на пост Госсекретаря и был его правой рукой в избирательной кампании. Поэтому, при всем различии стиля руководства с Х. Клинтон, Дж. Керри в конечном счете пытается реализовывать все ту же концепцию «умной силы» в интересах наднациональных элит.

Возникает вопрос, почему же при очевидных неудачах практической реализации концепции «умной силы», она продолжает использоваться в качестве идейной основы внешней политики США.

Представляется, что ответ заключен в следующем обстоятельстве. Жители любой страны, что Америки, что России, что Китая искренне полагают, что их страна является главным пунктом повестки дня для всех стран мира. Однако в те или иные периоды времени это оказывается не вполне так. Дж. Керри, если судить по основным публикациям «думающих танков», отражающих позиции тех или иных политэкономических элитных групп – это в значительной мере, что называется «технический» госсекретарь. Вместе с Б. Обамой он призван до 2016 года реализовать две главных глобалистских задачи. Речь идет о создании Трансатлантического торгового и инвестиционного партнерства и Транстихоокеанского торгового партнерства. В Трансатлантическое партнерство должны войти США, Мексика, Канада, т. е. страны

НАФТА и страны ЕС. А в Транстихоокеанское партнерство, как предполагается, войдут все те же страны НАФТА, ряд стран Латинской Америки, Япония, Южная Корея, Австралия, Новая Зеландия и еще ряд стран Южной и Юго-Восточной Азии.

Смысл этих партнерств достаточно прозрачен. Они призваны унифицировать различного рода торговые правила, технические и иные регламенты и другие нормативные документы, связанные с ведением бизнеса, использованием информации и т. п. Вместе с отсутствием каких-либо таможенных и иных экономических барьеров, формирование этих партнерств образует своего рода огромную единую технологическую, производственную, финансово-экономическую и в значительной степени политическую зону.

Для реализации именно этой задачи, в которой максимально заинтересованы все крупнейшие корпорации, доктрина «умной силы» с акцентом на коллективные действия, использование активистских групп и наличие единой неолиберальной идеологии, подходит как никакая другая.

Есть основания полагать, что на все другие международные события последнего периода, включая события на Ближнем Востоке, на Украине, в Южной Азии и т. п., верхушка мировой наднациональной элиты смотрит именно с позиции их использования для снятия препятствий и ускорения процессов подписания соответствующих соглашений, которые намечены на 2015 год. А соответственно амери-

канское внешнеполитическое ведомство реализует не столько национальные интересы, сколько обслуживает глобалистскую иерархо-сетевую структуру, в основе которой находится кластер крупнейших финансовых институтов и транснациональных корпораций.

При этом если еще 20–25 лет назад внешняя активность США могла распространяться на целый ряд регионов, где они осуществляли наступательные, по большей части эффективные действия, то в последние 10–15 лет картина коренным образом изменилась. Страна либо пытается ликвидировать последствия внешнеполитических неудач, типа авантюр в Ираке и Афганистане, либо, как уже отмечалось выше, обслуживает интересы наднациональных структур. Такое положение в немалой степени усугубилось принятием на вооружение доктрин «мягкой», а затем «умной» силы Дж. Ная.

Каждая доктрина имеет обязательно ключевой инструмент реализации. А этот инструмент в свою очередь предполагает вполне практическую, понятную форму своего действия.

В последние 10 лет сошлось так, что доктрина «мягкой силы» вызвала к жизни целый ряд инструментов и форм, которые будучи крайне многообещающими на первый взгляд, оказались совершенно провальными на практике.

Прежде чем детальнее рассмотреть, о чем конкретно идет речь, надо отметить, что такое положение является ярким

свидетельством уменьшения калибра ключевых фигур на американской политической сцене. Оно же демонстрирует и снижение уровня проработки важнейших внешнеполитических решений.

Сегодня сложилась достаточно парадоксальная ситуация, когда «фабрики мысли» продолжают повышать уровень своей работы, корпорации и отдельные государственные и надгосударственные структуры, в первую очередь, в разведывательном сообществе используют все более изощренные инструменты, а на высшем государственном уровне делаются удивительные по своей нелепости просчеты.

Инструментом реализации политики «мягкой», а затем «умной» силы стала концепция и инструментарий так называемого «управляемого хаоса», разработанные Стивеном Манном. Стивен Манн собственно не скрывал, что его концепция «управляемого хаоса» есть механизм практической реализации построений Дж. Ная. В одной из своих ключевых работ он прямо писал: «Конфликтная энергия заложена в основы человеческих свойств с того момента, когда индивидуум стал базовым блоком глобальных структур. Конфликтная энергия отражает цели, ощущения и ценности индивидуального актора – в сумме, идеологическое обеспечение каждого из нас запрограммировано. Изменение энергии конфликта людей уменьшит или направит их по пути, желательному для наших целей национальной безопасности, поэтому нам нужно изменить программное обеспечение. Как

показывают хакеры, наиболее агрессивный метод подмены программ связан с «вирусом», но не есть ли идеология другим названием для программного человеческого вируса?

С этим идеологическим вирусом в качестве нашего оружия, США смогут вести самую мощную биологическую войну и выбирать, исходя из стратегии национальной безопасности, какие цели-народы нужно заразить идеологиями демократического плюрализма и уважения индивидуальных прав человека».

Стивен Манн искренне полагал, что при помощи подобного программирования можно либо «отложить создание критического состояния, либо поощрить его, и направить развитие системы в нужное русло». При этом, «в действительности, сознаем это или нет, мы уже предпринимаем меры для усиления хаоса, когда содействуем демократии, рыночным реформам, когда развиваем средства массовой информации через частный сектор».

Особо следует подчеркнуть, что Стивен Манн не имел ни математического, ни физического образования, а был специалистом по английской классической литературе, который затем перешел на дипломатическую работу. Стивен Манн был карьерным дипломатом, близким Пентагону. Впервые прикладная концепция Стивена Манна была обнародована спустя два года после опубликования первых работ по «мягкой силе» в 1992 году в журнале Военного колледжа армии США, в томе 22 под названием «Теория хаоса и стратегиче-

ская мысль». Кроме своей основной работы несколько позже он опубликовал работу «Теория сложности и политика национальной безопасности» в книге «Сложность, глобальная политика и национальная безопасность», изданной Университетом национальной обороны.

В своих статьях, посвященных прикладным аспектам теории хаоса, он обслуживал новую пентагоновскую стратегию, связанную с крахом Советского Союза. Эта стратегия впервые была опубликована в марте 1992 года и утверждена еще президентом Джорджем Бушем-старшим. Стратегия предусматривала, что «первая и главная цель стратегии состоит в том, чтобы предотвратить повторное появление любой новой сверхдержавы на территории бывшего Советского Союза или в каком-либо другом месте. Цель состоит в том, чтобы Соединенные Штаты Америки никогда впредь не сталкивались с угрозой, сравнимой с Советским Союзом. Это является главным фактором, лежащим в основе новых глобальных и региональных стратегий. Практически они должны обеспечить условия, которые предотвратят доминирование любой враждебной силы в регионах, ресурсы которых достаточны для создания в перспективе новой глобальной власти. К таким регионам относятся Западная Европа, Восточная Азия, территории бывшего Советского Союза и Юго-восточной Азии». (Выдержки из «Руководства Пентагона по предотвращению повторного появления нового соперника», опубликованные газетой New York Times 08.03.1992 г.)

Прикладная теория управляемого хаоса Стивена Манна как раз и была призвана предоставить инструментарий для деструкции территорий и ресурсных баз потенциальных кандидатов в новые сверхдержавы. В первые годы после своего появления теория в основном не выходила за пределы государственного департамента и учебных учреждений министерства обороны США. Ситуация изменилась с приходом к власти администрации Дж. Буша-младшего. Политические авантюристы и, как впоследствии выяснилось, распильщики военных бюджетов и коррупционеры Р. Чейни и Д. Рамсфелд всерьез восприняли дилетантские построения Стивена Манна. Это тем более удивительно, что именно в Соединенных Штатах расположен Институт сложности в Санта-Фё, который является одним из мировых лидеров в сфере изучения нелинейных, неравновесных процессов. Более того, Стивен Манн выступал несколько раз там со своей концепцией и был жесточайшим образом раскритикован. В результате дилетантизма, воцарившегося в Вашингтоне в последние десятилетия, пропагандист-популяризатор последовательно направлялся на работу в ряд ключевых горячих точек. Итоги говорят сами за себя.

Подавляющая часть проблем, с которыми сталкиваются в настоящее время Соединенные Штаты в самых разных уголках планеты, от Египта до Пакистана, от Бразилии до Афганистана, является результатом их же собственных неразумных, авантюристических действий, в значительной степени

связанных с реализацией стратегии «управляемого хаоса». Т. е. сегодня огромные финансовые ресурсы и усилия тратятся на борьбу с собственными ошибками и просчетами.

Не надо быть работником ведущей «фабрики мысли» или выпускником MIT для того, чтобы понять простую вещь. Теория хаоса – это не что иное, как общеупотребительное название теории динамических, стохастических, нелинейных систем. Отличительной особенностью этой теории является тот факт, что она научилась выделять широкий круг существующих в природе и обществе систем и процессов, которые характеризуются высокой неустойчивостью и неопределенностью. Как правило, эти характеристики присутствуют не всегда, а появляются лишь на определенной стадии существования системы. Эти стадии называют еще «самоорганизованной критичностью», «режимом с обострением», «повышенной турбулентностью» и т. п. Названия разные, но суть одна. Будущее таких систем практически невозможно предсказать. Более того, выбор того или иного варианта дальнейшего существования системы в немалой степени случаен. Еще более важно то обстоятельство, что малые воздействия на систему порождают очень большие последствия. Причем, как говорят математики, зависимость между функцией и аргументом имеет не одно, а много решений. Т. е. оказывая малое воздействие, никогда наперед не знаешь, какой будет результат.

В общем, всё это азы математики, синергетики, теории

сложности. Однако в мире, где пропагандисты выступают в роли аналитиков и обслуживают дилетантов-политиков, незнание базовых принципов используемых методов чревато разрушительными последствиями. Собственно, это мы и можем наблюдать во многих внешнеполитических акциях США последнего времени.

Любой выпускник приличного университета или человек, поварившийся в бизнесе, военном деле, или побывавший в горячих точках, если ему задать вопрос об управляемом хаосе, не колеблясь, ответит, что речь идет об оксюмороне. Хаос можно организовать или вызвать, но управлять им еще никто не научился. Ведь хорошо известно, что управляющая система для того, чтобы осуществлять эффективное управление, по сложности должна превосходить управляемую. А это условие, применительно даже к самым простым обществам, выполнить крайне сложно. Поэтому после каждого вмешательства американцев остаются фейл стейт и зоны перманентных боевых действий, типа Сомали, Йемена, Афганистана, других стран Ближнего Востока, лесных районов Колумбии и т. п. В свою очередь, в последующем эти регионы становятся рассадниками мирового терроризма, наркотрафика, работорговли, торговли оружием и т. п. В общем, концепция управляемого хаоса обернулись вторжением хаоса в сами Соединенные Штаты.

Надо сказать, что американский истеблишмент, несмотря на множество сложностей и недостатков, способен быст-

ро учиться на собственных ошибках и извлекать уроки не только из чужих, но и из своих неудач. Поэтому в начале десятых годов теория Стивена Манна стала подвергаться уничтожающей критике в самих Соединенных Штатах, и была фактически снята с вооружения в качестве одного из основных внешнеполитических методов.

Встречающееся среди многих российских экспертов мнение, что события «арабской весны» и война в Сирии являются порождением стратегии управляемого хаоса, реализованной Соединенными Штатами Америки, не имеет сколько-нибудь солидного документального фактологического подтверждения. Природа этих событий носит несколько иной характер, рассмотрение которого выходит за пределы настоящей работы.

Еще одним до поры до времени эффективным методом реализации стратегий «мягкой», а затем «умной» силы были «оранжевые» революции, базировавшиеся в первую очередь на комплексе работ Джина Шарпа. Фактически Джин Шарп поставил перед собой задачу классифицировать, кодифицировать и привязать к конкретным ситуациям все наблюдавшиеся в истории методы ненасильственных действий. В итоге, в своей работе «Power and Struggle (Politics of Nonviolent Action, Part 1)» («Власть и борьба (Политика ненасильственных действий, часть I»), изданной еще в 1973 году он выделил 198 методов ненасильственного протеста и убеждения.

Хорошо известны примеры «оранжевых» революций и

роль американских и британских внешнеполитических разведывательных ведомств в их подготовке и практическом осуществлении. Гораздо менее известен тот факт, что в настоящее время революционный конструктор Джина Шарпа стал предметом критического рассмотрения.

Летом 2013 года в ведущем учебном центре по подготовке специалистов по «оранжевым» революциям, во Флетчеровской школе Университета Тафтса, США совместно с ведущим центром по разработке методов сопротивления власти – Международным центром по ненасильственным конфликтам (ICNC) была проведена в полузакрытом режиме большая конференция «Ненасильственное сопротивление: вчера, сегодня, завтра».

Работа конференции была выстроена вокруг обсуждения доклада М. Стефан и Э. Ченовез «Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict». В докладе были изложены результаты статистического исследования всех гражданских конфликтов в мире за 1985–2013 годы. По итогам анализа выяснилось, что движения гражданского сопротивления добились успеха в 55 % зафиксированных случаев, в то время, как военные противостояния власти имели успех только в 28 %. В итоге был сделан вывод о том, что «гражданские ненасильственные кампании обеспечивают устойчивый переход к демократии в два раза чаще, чем вооруженное противостояние с властью».

Однако наряду с этим привычным выводом, на конферен-

ции выяснилось, что в течение последних 15 лет наибольшую эффективность показали смешанные стратегии, которые имели успех почти в 70 % случаев. К смешанным стратегиям относились гражданские ненасильственные кампании, которые сопровождались либо угрозой силового противостояния с властью, либо с точечными конкретными вооруженными акциями. Соответственно был сделан вывод о необходимости разработки теории, а главное детального практического инструментария для гибридного гражданского сопротивления, включающего как ненасильственные методы, так и целевые вооруженные акции или угрозы применения силы против власти. Первым примером практической отработки подобного инструментария и технологий стали украинские события начала 2014 года.

Кроме того, на конференции было рекомендовано повысить эффективность гражданских ненасильственных кампаний за счет широкого использования новых информационных технологий, обеспечивающих улучшение координации, информирования и обеспечения совместных действий «гражданского сопротивления».

Приведенный документальный материал показывает, что к середине 2010-х годов концепция «умной силы», включая методы и формы ее реализации, в значительной степени исчерпала себя, по крайней мере, в своем первоначальном виде.

Помимо отмеченных ограничений в использовании ме-

тодов и форм реализации стратегии «умной силы», безвозвратно скомпрометирована сама основа этой стратегии. Дж. Най, давая в свое время формулировку источников «мягкой силы» в интервью журналу Шпигель, отмечал, что «во-первых, это культура страны – так, в Америке культурное поле простирается от Гарварда до Голливуда. Во-вторых, политические идеалы, которые могут быть очень привлекательными для других, – это и демократия, и принцип свободы слова, и равенство возможностей. В-третьих, легитимность внешней политики, под которой понимается такой образ действий правительства, который другие народы могут признать соразмерной защитой наших национальных интересов».

Вряд ли кто сегодня будет спорить о том, что практически все три указанных источника, что называется, полностью пересохли. В условиях перехода к широкополосному дешевому интернету Голливуду нанесен едва ли не смертельный удар. В отличие от восьмидесятых – нулевых годов практически во всех основных странах мира налицо подъем национального телевизионного кинематографа, широкая экспансия компьютерных игр, а также других национальных культурных продуктов. Что касается равенства возможностей, то сегодня это самими американцами воспринимается как издевка. В США сегодня один из самых высоких в мире уровней неравенства. Уже долгие годы все хуже работают социальные лифты. Американская мечта о чистильщике обу-

ви, ставшим миллиардером, осталась лишь в воображении только что подключившихся к интернету жителей африканской саванны или австралийских аборигенов. С такой же, по меньшей мере, иронией воспринимается легитимность внешней политики США, которая в текущем веке прошла достаточно бесславный путь от иракской и афганской авантюр до разоблачений Сноудена.

В сложившейся ситуации американские элиты и наднациональные глобалистские сети в значительной мере господствующие и паразитирующие на Соединенных Штатах, заняты разработкой принципиально новых действенных инструментов эффективного и по возможности экономичного решения проблем устранения геополитических противников и формирования глобалистского пейзажа мира.

2.2. Стратегия и тактика превентивных действий

В условиях острого запроса на новые методы борьбы с государственностью наиболее рекламируемым, популярным и доступным для внешнего наблюдения и анализа направлением остается модернизация инструментария, разработанного Джином Шарпом. Сегодня эта работа ведется в международном масштабе в рамках инициативы Civil Resistance 2.0: A New Database of Methods. Целью инициативы является аккумуляция всего мирового опыта использования информационных технологий при осуществлении антиправительственных ненасильственных действий. Наконец, в рамках инициативы собранные методы дорабатываются профессионалами в области информационных, когнитивных и социальных наук и практик, а затем транслируются так называемым гражданским активистам по всему миру.

Инициатива реализуется на базе Вашингтонского университета в Сиэтле, в рамках Digital Activism Research Project (DARP). Финансируется проект имеющим теснейшие связи с военно-разведывательным сообществом Национальным научным фондом США, подведомственным Госдепартаменту Институтом мира США и Фондом Макартуров, одним из главных спонсоров некоммерческих активистских организаций по всему миру. Ежегодно проект выпускает подробней-

шую базу данных по методам и инструментам цифрового сопротивления или цифрового активизма. В последнем отчете, опубликованном в 2013 году, обобщено более 400 компаний цифрового активизма из 100 стран за период 2010–2012 годы. Помимо фактического материала для так называемых цифровых активистов доступны усовершенствованные специалистами своего рода методические рекомендации и инструкции по использованию доработанных наиболее эффективных инструментов цифрового сопротивления. Доклады и материалы обновляются ежегодно.

При всей важности этой работы представляется, что, в конечном счете, она является одновременно своего рода переходной стадией и операцией прикрытия для формируемых в настоящее время принципиально новых, взаимоувязанных стратегии, тактики и оперативных мер, обеспечивающих соответствующим инструментарием для борьбы с властью и дестабилизации общественного порядка в странах-противниках глобалистской наднациональной элиты.

Поскольку данная работа находится в полном разгаре, было бы трудно ожидать появления законченных монографий на этот счет. Более того, есть все основания полагать, что такие монографии вообще не будут написаны. Дело в том, что само по себе очерчивание той или иной стратегии с системой мер по ее реализации, как показывает опыт, снижает эффективность ее применения. В зарубежных источниках содержится множество указаний на то, что последние несколь-

ко лет многие исследования в области социальных, военных, когнитивных наук полностью или частично секретятся.

Однако анализ всей совокупности исследовательской активности ведущих научных центров и университетов, повесток дня проводимых конференций, а также финансируемых из государственных источников, прежде всего США, исследований и разработок, позволяет очертить не только общую направленность, но и основные блоки формирующейся политики и инструментария борьбы с государственностью и деструкции геополитических субъектов.

Для формирования методологической основы зарождающейся концепции огромное значение имела недавно изданная книга Барнетта Р. Рубина «Blood on the Doorstep. The Politics of Preventive Action». Автор является ведущим исследователем Нью-Йоркского университета и одной из ключевых фигур в чрезвычайно влиятельном Совете по международным отношениям.

Книга написана в основном на материале кровопролитных конфликтов последних 20 лет. Цель работы – это проработка теоретического, практического и даже юридического фундамента для превентивных действий в отношении независимых государств. Логика книги состоит в следующем. Многие конфликты, унесшие тысячи человеческих жизней, по мнению автора, произошли потому, что Запад, скованный различного рода международными соглашениями, вовремя не вмешался и не положил конец насилию на раннем этапе

конфликта. Отсюда делается вывод о том, что для предотвращения потенциально «большой крови» вполне оправдано и справедливо насильственное вмешательство или прямая поддержка вооружением и инструкторами для боевиков извне на самой ранней стадии конфликта, в сочетании с гражданским ненасильственным сопротивлением изнутри. При этом, поскольку государства обременены множеством соглашений и условий международного права, то такие превентивные действия, по мнению автора, могут выполнять, в том числе, негосударственные, частные или некоммерческие организации. Хотя книга написана практически полностью на материале Азии и Африки, последние два года Б. Рубин на многих конференциях отстаивает точку зрения, что предлагаемый им подход носит универсальный характер. Причем его точка зрения находит все большее и большее понимание в официальных кругах Соединенных Штатов, Великобритании и ряда европейских стран.

Этому в значительной мере способствует недавно появившееся и с каждым годом крепнущее идеологическое течение, которое исходит из превосходства Запада над всеми иными цивилизациями. Если С. Хантингтон в своей знаменитой работе «Столкновение цивилизаций» исходил из наличия нескольких конфликтующих независимых, но в каком-то смысле равных цивилизаций, то новое течение фактически утверждает, что существует только западная цивилизация и варвары, которые к ней, в конечном счете, долж-

ны присоединиться.

Экономическое обоснование этой концепции сделано в наиболее популярном экономическом труде последних пяти лет «Why Nations Fail: The Origins of Power, Prosperity, and Poverty». Его авторы Д. Асемоглу и Д. Робинсон, несмотря на молодой возраст, являются наиболее вероятными кандидатами на получение Нобелевской премии по экономике в ближайшие годы. Книга блестяще написана, базируется на огромном фактическом материале и переведена на основные языки. Главный ее смысл состоит в том, что только западные экономические институты способны обеспечить экономическое развитие и социальный прогресс.

Историческое обоснование концепции исключительности Запада сделано в книге Н. Фергюссона «Civilization: The West and the Rest». На русский язык название книги можно перевести, как «Цивилизация: Запад и все остальные». В книге отстаивается концепция, смысл которой в следующем: только на принципах западной, преимущественно британской цивилизации может быть построено нормальное общество. Запад является, по мнению автора, абсолютно уникальным феноменом в истории человечества. Соответственно для остальных цивилизаций единственный шанс на выживание это – ассимиляция в западную, а точнее англо-американскую цивилизацию. По мнению Н. Фергюссона, в противном случае будет происходить не столкновение цивилизаций, как полагал Хантингтон, а «сокрушение цивилиза-

ций, не ассимилировавшихся с Западом».

Н. Фергюссон в течение последних лет входит в число 100 наиболее авторитетных и известных на Западе мыслителей. Он является профессором Гарвардского университета, советником руководства республиканской партии США.

По мнению Н. Фергюссона гражданский активизм и протестные действия в странах, не относящихся к западной цивилизации, всегда направлены на то, чтобы перейти от состояния фактического варварства к цивилизованному строю, т. е. приобщению к англо-американской цивилизации. Поскольку зачастую власти стран, где действуют гражданские активисты, препятствуют им в ненасильственных действиях по включению в единую и единственную западную цивилизацию, то это чревато в перспективе кровопролитными конфликтами. Соответственно, Запад, по мнению Н. Фергюссона, вправе, чтобы предупредить эти конфликты, осуществить превентивные действия, включая поддержку извне, как ненасильственных кампаний, так и насильственных акций сил сопротивления.

Указанные выше работы представляют своего рода идеологический базис и обоснование новой стратегии превентивных действий.

Вместе с концепцией управляемого хаоса в последние годы критически переосмыслена и, по сути, утратила влияние концепция «умной толпы», впервые описанная в книге H. Rheingold «Smart Mobs: The Next Social Revolution». Дело в

том, что даже хорошо технически оснащенная и информатизированная толпа остается толпой, т. е. крайне малоуправляемым, нестабильным и неорганизованным формированием.

В последние полтора года прошел целый ряд конференций, участники которых пришли к выводу, что концепция «умной толпы» построена на значительных преувеличениях. Дело в том, что данная концепция в значительной степени сформировалась под влиянием уличных бунтов и беспорядков в Великобритании, Франции, Германии и т. п. Было отмечено, что по факту все эти события носили локальный характер, охватывали, в общем, незначительное число участников и не имели по сути никаких политических последствий. При этом на конференциях эти бунты противопоставлялись событиям «парижской весны» 1968 года, движению против войны во Вьетнаме в конце 60-х и др. подобным акциям, которые затрагивали сотни тысяч и даже миллионы людей.

Однако в современном индивидуализированном мире попытка реанимировать технологии, лежавшие в основе этих движений, обречены на неудачу. Поэтому в качестве стержня концепции превентивных действий предлагается использовать прежде всего политтехнологическое наследие Сола Алинского.

Этому в значительной степени способствовало и то, что учеником Сола Алинского являлся политтехнолог номер один в Соединенных Штатах Касс Санстейн. В системе С.

Алинского несколько лет работал Барак Обама. Диплом по работам С. Алинского писала Х. Клинтон, которой в двадцатилетием возрасте С. Алинский предсказал блестящее политическое будущее.

В России ни одна из книг С. Алинского до сих пор не издана. Поэтому есть смысл более подробно остановиться на сути его концепции. С. Алинский начал свою практическую работу в 30-е годы и вел до самой смерти в начале 70-х. После его смерти продолжают действовать многочисленные организации, построенные на идеях С. Алинского, его разработки активно используются политтехнологами Демократической партии США.

Главным содержанием как книг, так и практической деятельности С. Алинского были методы захвата власти для осуществления преобразований. В своей главной книге «Rules for Radicals» («Правила для радикалов») С. Алинский пишет: «Достоевский считал, что больше всего люди боятся сделать первый шаг. Поэтому любому революционному взрыву должно предшествовать медленное, пассивное изменение сознания людей, в результате чего они должны почувствовать себя настолько неприкаянными, отвергнутыми, потерянными и бесперспективными в господствующей системе, что сами начнут желать отпустить прошлое и изменить будущее. Для любой революции важно желание масс принять преобразование. Чтобы создать такую ситуацию, организатор должен работать не только со средним классом, но

и с «голубыми воротничками», иначе они сдвинутся вправо. Этого нельзя допустить». Но у бедных нет никакой власти, поэтому реальной целью должен быть средний класс: «Сейчас и в последующих десятилетиях организация должна сосредоточить свои действия на среднем классе. Это – то место, где концентрируется власть…»

Следует отметить, что под средним классом С. Алинский понимал не офисных бездельников и представителей новой богемы, а, прежде всего, людей дела – инженеров, конструкторов, линейный персонал в фирмах, банках и других организациях.

С. Алинский понимал, что люди дела, у которых есть определенный достаток с одной стороны, а с другой стороны – навыки практической работы, вряд ли горят желанием вступать в конфронтацию с властью. Поэтому прекрасно зная труды Г. Лебона, Г. Тарда и других, С. Алинский делал ставку не на толпу, а на организацию. Он полагал, для того, чтобы бороться с властью, на первом этапе надо ставить совершенно приземленные, конкретные, бытовые цели. На этом этапе он ставил задачу объединить людей, живущих в одном районе, организовать вокруг общих для них проблем и втолковать, что им нужно сообща финансировать их решение. В свою очередь решение предполагает создание сильной структуры – своего рода кооператива по решению проблем отдельно взятого района – способного к долгосрочной работе.

При этом он отдавал себе отчет, что сам народ организоваться не в состоянии. Для этого ему нужен специально подготовленный, обученный и натренированный организатор. Организатор должен, во-первых, обладать необходимыми знаниями и недюжинным умом, во-вторых, длинной волей и сильным характером, и, в-третьих, иметь суггестивные способности, и быть обученным методам успешного манипулирования людьми и организационной работе. Т. е. ключевой фигурой в концепции С. Алинского был организатор.

Готовились организаторы в специальных школах, открываемых, как правило, при университетах. Наиболее активно эта работа развернулась в Чикаго, включая Чикагский университет, где с системой С. Алинского познакомились Б. Обама, К. Санстейн и др.

При подготовке организаторов С. Алинский сформулировал правила, которые они должны реализовать в своей работе. Эти правила изложены в его главных книгах «Rules for Radicals» и «Reveille for Radicals». В число важнейших правил входят следующие:

• Медленно проникайте, просачивайтесь в такие существующие организации как церкви, профсоюзы, политические партии и т. п. Скрытно добивайтесь влияния внутри этих организаций и затем начинайте перемены с этой платформы.

• Полностью поддерживайте людей в их недовольстве и разногласиях.

• Используйте провокационные вопросы, чтобы манипулировать и использовать людей для предварительно заданной программы. Раздувайте напряжённость между ними как можно сильнее.

• Организатор должен вызвать на себя атаку, которая затем закрепит доверие к нему людей.

• Врага народа необходимо обозначить и назначить персонально.

• Враг должен быть совершенно поляризован, 100 % негативно, как первопричина полного поражения или полной победы.

• Цель оправдывает средства.

• Радикал нацеливается на средний класс, так как он самый большой, и смешивается с ними, говорит на их языке, одевается, как они, использует их нравы, обращается к их моральным принципам.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, купив полную легальную версию на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.