НИКОЛАЙ ИВАНОВ

КИБЕРТЕРРОР И КИБЕРВОЙНА В СОВРЕМЕННОМ МИРЕ

– Русские хакеры подтасовали результаты президентских выборов в США, привели к власти Трампа, пытались избрать "агентов Кремля" президентами Франции, Германии, Австрии, Литвы и других стран!

– Россия ведёт полномасштабную кибервойну! – кричат западные политики, журналисты, "эксперты" со всех сторон.

– Наступил "кибернетический Пёрл-Харбор", а мы его проспали!

– Они на расстоянии взламывают айфоны западных политиков и считывают их конфиденциальные данные!

– Они украли десятки миллиардов долларов со счетов крупнейших западных банков!

В чёрной пропаганде о "злобных русских хакерах" эксплуатируется страх потери "чудесных" достижений последнего времени. Миф о "воплощённой техноутопии", "сказочном техническом прогрессе", сопровождаемом ежегодной сменой новейших компьютерных систем и "гаджетов", является в настоящее время главной подпоркой дряхлого, умирающего империализма. Благодаря компьютеризации значительная часть информации, включая государственные и корпоративные секреты, хранится сейчас в электронном виде, на компьютерах, подключённых к интернету. Большая часть мировых финансов находится на виртуальных, электронных счетах, и там же проходят все финансовые потоки по заключённым сделкам. Материальная инфраструктура (предприятия, транспорт, энергетика и проч.) контролируются в автоматическом или полуавтоматическом режиме компьютерами. Возможности выхода на все эти системы через интернет весьма соблазнительны для различных злоумышленников. Американцы, естественно, боятся потерять это богатство, и на этих фобиях играет пропаганда, создавая новый тип "всемирного злодея" – безумного русского хакера, ставящего своей целью уничтожить "прекрасный цветок американской цивилизации".

Но в настоящее время создаётся впечатление, что "перехлёсты" в этой пропаганде превысили все разумные рамки, что все эти респектабельные политики и журналисты просто "слетели с катушек"! Подобного массового психоза, по высочайшему накалу эмоций и полному отсутствию каких-либо доказательств, не было в современной истории. С ним не может сравниться даже печально известная "охота на ведьм" сенатора Маккарти в начале 50-х годов, когда параноики из сенатской комиссии обвинили, изгнали и посадили в тюрьмы тысячи госслужащих США по подозрению в "связях с коммунистами".

Мудрый русский народ давно заметил причину подобного визга. Кто громче всех кричит: "Держите вора!"? Сам же вор.

Волну психоза удалось несколько сбить только после недавней публикации известным сайтом *WikiLeaks* (Дж. Ассанж) тысяч секретных документов ЦРУ, раскрывших истинные гигантские масштабы кибертерроризма, который ведётся спецслужбами США.

Первый выпуск под названием "Нулевой год" состоит из 8761 документа, добытых из Центра киберразведки ЦРУ (Лэнгли, штат Вирджиния). *WikiLeaks* не указывает источник информации, однако ясно, что это подлинные, достоверные файлы об использовании хакерских и иных инструментов для заражения многочисленными вирусами компьютерных систем противника (прежде всего России); для создания "закладок", для возможности создать в определённый момент хаос в электронных схемах и системах управления, привести к катастрофам на автомобильном и авиатранспорте; для взлома систем компьютерной безопасности, баз данных и персональных файлов государственных органов и интересующих ЦРУ людей; для внесения хаоса в финансовую систему противника; для внедрения электронных "бомб с часовым механизмом", рассчитанных на срабатывание через определённый промежуток времени; для сбора различной развединформации через все известные на настоящий момент электронные "гаджеты", включая телефоны, компьютеры и телевизоры.

Самое активное сотрудничество американским спецслужбам было оказано компаниями *Apple*, *Google*, *Microsoft* и *Samsung*. Они предоставили свои собственные профайлы на всех известных в мире деятелей, политиков, журналистов, включая персональные данные, анализ привычек и пристрастий, адреса и пароли электронной почты и прочее.

В киберразведке ЦРУ применяются новейшие методы разрушения и проделывания "дыр" в защитных электронных системах, незаметного для противника "обхода" антивирусных программ, нанесения ударов по компьютерным научным центрам и институтам (включая лабораторию Касперского в России). Активная кибервойна ведётся также против национальных предприятий, пытающихся создать автономные, независимые от Запада компьютерные системы и устройства.

Чужеродные "закладки" находятся в айфонах, айпадах, смартфонах на базе популярной платформы *Google Android*, ноутбуках, десктопах и лэптопах, работающих с операционной системой *Microsoft Windows*. Согласно опубликованной информации, главные центры кибертерроризма находятся в штабквартире ЦРУ в Лэнгли, а также в консульстве США во Франкфурте-на-Майне (Германия).

Хакеры, взламывающие банки, запускающие вирусы, совершающие акты диверсий, как оказалось, действуют отнюдь не сами по себе. Более того, им выдают американские дипломатические паспорта, они могут без таможенного досмотра путешествовать по всему миру и разворачивать подрывную деятельность из любой точки земного шара.

Сбор развединформации киберспецами ЦРУ идёт не только через прослушку персональных устройств пользователей и взлом электронной почты, но и через популярные социальные сети – *Facebook*, *Instagram*, – известные приложения *WhatsApp*, *Signal* и *Telegram*.

Некоторые из добытых файлов содержат данные об использовании электронных "закладок" в автомобилях для *VIP*-персон и самолётах, которые позволяют не только прослушивать разговоры, ведущиеся в салоне, но и в определённый момент "перехватывать" управление автомобилем (самолётом) для совершения теракта, закамуфлированного под "случайную катастрофу".

Документы *WikiLeaks* вскрывают взаимосвязь всех разведслужб США в добыче и анализе полученной информации, а также привлечении к работе секретных служб Англии, Австралии, Канады и Новой Зеландии.

Все вышеуказанные действия американские эксперты относят к мягкому понятию "киберразведки". Но вот "кибертерроризм", по их словам, это, конечно, работа "русских хакеров"!

Какое же определение дают сами американцы кибертерроризму? Это "заранее спланированные, политически мотивированные атаки, направленные против информационных, компьютерных систем, компьютерных программ и баз данных, которые приводят к существенному материальному ущербу, жертвам среди мирного населения, созданию обстановки хаоса и паники". В отличие от "обычной киберпреступности" (распространения зловредных вирусов, локальных хакерских атак, завершающихся отказом компьютерного

оборудования отдельных пользователей или воровством денег с электронных банковских счетов), кибертерроризм, по определению ФБР и ЦРУ, "наносит существенный ущерб всему населению или его значительной части; согласованные действия террористов направлены на вывод из строя системы финансового и денежного обращения, военных объектов, электростанций, диспетчерских центров аэропортов, транспортных артерий и систем водоснабжения, компьютерных сетей и интернета".

Ясно, что различие между определениями "кибертерроризма" и "киберпреступности" довольно расплывчатое, так как ограбление банков и частных лиц хакерами из спецслужб США может быть частью систематической кампании террора в отношении государства-"мишени". Таким образом, кибертерроризм – это, прежде всего, намеренное использование компьютеров, интернета и локальных сетей для нанесения максимального ущерба противнику и отдельным лицам, занимающим в государственных органах высокое положение.

Но ведь это определение, как следует из документов *WikiLeaks*, полностью соответствует кибератакам, совершаемым в последние десятилетия правительством и спецслужбами США.

Правительство, Пентагон и ЦРУ с восторгом восприняли идею войны с помощью вредоносных вирусов и компьютерных технологий, направленных против России и других "стран-изгоев". Главным преимуществом нового вида оружия стала полная безнаказанность – ведь проследить источник атаки и доказать причастность к нему государственных структур США практически невозможно.

Конечно, разведка и военные постоянно раздували "русскую угрозу" кибератак, преувеличивая возможности российских специалистов.

Эксперты в компьютерной сфере утверждали, что размах "угрозы" фантастически преувеличен, и россияне вряд ли в ближайшее время смогут причинить какие-либо неприятности кибербезопасности США. Но пу́гало "русских хакеров" было необходимо для выбивания всё новых бюджетных средств на кибертерроризм. Президент Обама, руководители Пентагона и ЦРУ постоянно заявляли об "угрозе кибератак со стороны России" (и в меньшей степени – Китая). В их взвинченных до истерики выступлениях указывалось, что "практически все системы, жизненно важные для безопасности государства, уязвимы для внешних кибератак, которые могут нанести колоссальный финансовый и материальный ущерб стране".

В 2000-е годы были попытки свалить на "русских" некоторые крупные аварии на американских предприятиях, но эксперты и следователи не смогли представить ни малейшего доказательства.

В 2010 году заместитель министра обороны У. Линн выступил с "сенсационными разоблачениями", обвинив русских в кибератаках на серверы Пентагона, ЦРУ и других спецслужб. "Каждый день, – заявил он, – военные и гражданские сети подвергаются атакам тысячи раз и сканируются миллионы раз; наши противники смогли незаконно выудить тысячи секретных файлов из серверов государственных учреждений США и их союзников, а также военно-промышленных корпораций, включая чертежи, оперативные планы и разведданные".

Использовав эту фальшивку, поддержанную президентом Обамой, и под невероятный пропагандистский визг о "русской угрозе" в 2011 году в министерстве обороны была создано специальное "Кибер-Командование" (Кибер-Ком), получившее статус "пятого рода войск" (наряду с армией, ВВС, ВМФ и космическими силами) и равное по своему положению региональным командованиям ВС США.

В истории человечества всегда, когда появляются новые виды вооружений и новые технологии, это даёт преимущества одной из стран (группе стран), которыми они сразу же стремятся воспользоваться и расширить свою власть и господство над теми "неудачниками", которые не сумели должным образом подготовиться к новой войне. Создание океанских судов и появление огнестрельного оружия позволило европейским странам захватить почти весь мир и превратить эти территории в зону своего колониального владычества, безудержной эксплуатации, беспощадного насилия и работорговли.

Изобретение танков, подводных лодок, пулемётов, отравляющих газов стало непреодолимым соблазном для начала Первой мировой войны, приведшей к краху главных монархических режимов Европы. Создание ядерного

оружия и его чудовищное "испытание" на мирных гражданах Хиросимы и Нагасаки на исходе Второй мировой войны породило эйфорию в правящей элите США и немедленно привело к разработке планов атомной бомбардировки СССР, союзника (!) в только что закончившейся мировой войне. Однако при тогдашней технологии потребовалось несколько лет, чтобы накопить достаточный арсенал подобного оружия. А за это время Советский Союз сумел ценой героических усилий создать своё собственное "оружие устрашения" и избежать страшной участи.

В настоящее время успехи в компьютеризации, интернет-технологиях (наряду с многочисленными изобретениями в области биологической, химической войны, новыми образцами космического оружия) также подогревают сладостные фантазии американских агрессоров. Многие из нынешних "ястребов", занимающих весьма влиятельные посты в американском истеблишменте, уже готовы "нажать все кнопки" в расчёте на то, что можно добиться победы над Россией в считанные часы.

В чистом виде кибервойна может привести к полному отключению страны от интернета (подобный эксперимент проводился американцами в отношении Северной Кореи в декабре 2014 года), одновременному использованию диверсионных "закладок" в компьютерном софте (а признаки подобных "бомб" были обнаружены европейскими экспертами в стандартных программах, используемых повсеместно в мире, например, в продукции компании *Microsoft*) для уничтожения хранящихся данных, организации сбоев в работе систем и даже причинения физического ущерба компьютерному "железу". Огромный урон может быть нанесён повсеместно, где используется американская техника с подобными "закладками", латентными вирусами и выходом в интернет – в промышленности, энергетике, на транспорте, в военной области, в космосе, финансово-денежном обращении.

Доклады американских экспертов по кибертерроризму показывают, что с помощью кибератак можно полностью вывести из строя оборудование ТЭЦ, атомных энергоблоков, гидроэлектростанций, электросетей (генераторы и трансформаторные станции), погрузив страну противника в темноту. Ущерб от подобных атак, способных лишить противника электроэнергии на длительный период, может быть сравним с материальными потерями воюющих стран во время Второй мировой войны

В 2010 году совместная американо-израильская кибератака была направлена против иранского ядерного предприятия в г. Натансе. Сложнейший вирус *Stuxnet* смог нанести непоправимый ущерб центрифугам, в которых (как полагал Моссад) происходит обогащение урана, направленное на создание иранской ядерной бомбы. Согласно израильским оценкам, кибератака задержала развитие иранской ядерной программы минимум на два года – гораздо больший срок по сравнению с возможным авианалётом (и с несравнимо меньшими потерями для израильтян).

Прямые кибератаки для нанесения ущерба инфраструктуре противника пока проводятся на экспериментальном уровне (хотя их возможности используются для сбора разведданных и "заметания следов" в интернете).

Для того, чтобы скрыть "государственный след" в применении кибероружия, используются индивидуальные хакеры и их сообщества подобно тому, как в XVI веке английская королева Елизавета I поощряла пиратов, давая им лицензии на "каперство" (безнаказанный грабёж и уничтожение испанских галионов).

Уличить эти частные группы или индивидуальных хакеров в связях с государством практически невозможно, и их используют в виртуальном пространстве подобно тому, как применяют полувоенные формирования "эскадроны смерти" или частные военные компании в обычных американских армейских операциях или карательных рейдах.

Спецслужбами США поощряется также хакерство с целью наживы, которое держит в постоянном напряжении банки и финансовые учреждения стран-"мишеней". Как специалисты из КиберКома, так и частные "подрядчики" ЦРУ и АНБ из числа хакеров используют в своих атаках "зомби-сети" компьютеров, заражённых вредоносным программами, DDOS-атаки на сайты (основной целью которых является выведение их из строя путём подачи огромного количества ложных запросов), вредоносные коды на вебсайтах, использование пиратского программного обеспечения, корпоративного шпионажа и краж через интернет личных данных.

Появились многочисленные наёмные хакерские группы, продающие свои услуги как частным лицам, так и государственным органам. Потери в мировом масштабе от их действий, по американским оценкам, составили более триллиона долларов только в 2009 году, как об этом официально заявил Обама, то есть прибыли этих "теневиков", работающих с подачи ЦРУ и других американских спецслужб, почти сравнялись с баснословными доходами от мировой продажи наркотиков. Конгрессмен Шелдон Уайтхауз объявил, что "прибыли кибермошенников превысили все доходы от воровства и пиратства за всю историю человечества".

Опять "указующий перст" американцев направлен на "русских и китайцев", хотя очевидно, что в этом высокотехнологичном "бизнесе" главную и определяющую роль играют американцы. Причём доходы от кибернетического разбоя идут, естественно, на счета главных грабителей с Уолл-стрит. Стратегическая линия на всемерное использование государственных и частных структур для организации кибервойн экономит колоссальные средства, которые необходимо затрачивать на обычные каналы добычи разведданных, а также на использование военной силы (спецназа, диверсантов и проч.).

В современном мире, где компьютерные системы с американской "начинкой" либо изготовленные по лицензии американских компаний используются на химических, атомных предприятиях, газопроводах, в диспетчерской системе аэропортов, на железнодорожных узлах возможности кибердиверсий практически неограниченны.

Есть сведения о том, что хакеры, спонсируемые американскими спецслужбами, устраивали "блэкауты" (повсеместные отключения электричества) в Бразилии в 2005-м, 2007-м и 2009 годах, в Венесуэле – регулярно в последние годы – для создания недовольства граждан левыми правительствами.

Однако при всём огромном ущербе, который может причинить кибертерроризм, он применяется только в совокупности с другими методами, которые в целом называют "информационной войной". Эти две ипостаси современной войны настолько связаны друг с другом, что довольно часто "кибертерроризм" во многих экспертных работах является синонимом "информационной войны". Одновременно используются кибератаки, "чёрная" и "серая" пропаганда, обычный терроризм (убийства известных политиков, дипломатов), кампании запугивания и шантажа, массового подкупа влиятельных лиц. Как и любая война, кибервойна направлена на разложение противника, создание прослойки предателей, подавление воли к сопротивлению, моральное закабаление народа. Активизация кибертерроризма обычно происходит в преддверии войны или организации государственного переворота.

В силу пассивной, "прагматической" позиции, занятой российским руководством по отношению к агрессии США в Ираке, а также из-за информационной блокады, установленной оккупантами, россиянам до недавнего времени практически ничего не было известно о кибератаках, предпринятых американцами в преддверии вторжения.

С начала 2000-х годов "американские хакеры" (на самом деле структуры ЦРУ и АНБ) использовали все известные на тот момент технологии кибертерроризма. Они основательно "почистили" счета иракских банков, устроили серию диверсий и актов саботажа, больно ударивших по экономике страны, внедряли вредоносные вирусы в жизненно важные системы управления, взламывали базы данных, прослушивали телефонные разговоры, ежедневно следили за политическими и военными деятелями страны. Важным техническим средством для осуществления кибертеррора стало использование DDOS-атак и перемаршрутизация (и последующее прекращение) интернет-трафика через американские фирмы.

С 2002 года мощные кибератаки сопровождались кампанией террора, шантажа, запугивания, направленной против иракской политической и экономической элиты. Используя новейшие достижения в области кибероружия, ЦРУ и Пентагон взломали и проникли в информационную систему госорганов Ирака и напрямую обращались к каждому из деятелей правящей партии БААС и военного командования, бомбардируя их факсами, электронными письмами и телефонными звонками, призывая устроить государственный переворот, выдавать США государственные и военные тайны (разумеется, на возмездной основе), приказывать войскам дезертировать после начала боевых действий и совершать другие действия, направленные на саботаж и подрыв власти Саддама Хусейна и иракского государственного аппарата.

Как только началась наземная операция, ВВС США стали наносить точечные удары, прежде всего, по государственным учреждениям и квартирам (виллам) тех представителей элиты, которые отказались сотрудничать с ЦРУ (по заранее утвержденному списку).

Невидимая кибервойна против правительства и военного аппарата Ирака была довольно успешной. Международная пресса сразу же после окончания боевых действий была переполнена историями о подкупе иракских военных и политических лидеров (включая коррумпированных чиновников и нефтяных олигархов), которые соглашались сотрудничать с ЦРУ и Пентагоном в обмен на обещание щедрой оплаты.

Одна из наиболее известных историй касается главы элитной Республиканской гвардии генерала Махера Суфьяна аль-Тикрити (близкого родственника Саддама). Он приказал своим частям прекратить сопротивление американским войскам после того, как, по его словам, заключил "денежное соглашение" с США.

Через месяц после окончания войны американский генерал Т. Фрэнкс (командующий Центральным командованием вооружённых сил США), ответственный за планирование и реализацию вторжения в Ирак, отметил: "Фактически с началом кибератаки 2002 года, то есть за год до начала операции "Шок и трепет", спецгруппы ЦРУ и Пентагона активно действовали на территории Ирака, подкупая чиновников, бизнесменов и генералов. У меня скопились горы расписок, в которых подкупленные иракские деятели давали письменное согласие работать на США".

Какими бы ни были прямые последствия этой подрывной деятельности США, вторичные последствия были ещё хуже. Учитывая специфику властной структуры правящей партии БААС, Саддам всегда больше всего боялся военного переворота. После того как США начали кибератаку, некоторые представители режима стали честно докладывать о том, что их пытаются подкупить американцы. Стали приносить эти послания в полицию или вышестоящему начальству.

Таким образом, иракский президент полностью осознавал масштабность американской операции, и это многократно усиливало его страхи. За несколько дней до начала войны он стал резко "закручивать гайки". Например, он запретил общение командующих дивизиями и корпусами между собой. Стал неожиданно перемещать генералов с одного места службы на другое. Для того чтобы противодействовать заговорщикам, президент поставил лидеров правящей партии БААС над военным командованием, причём приказы командиров любой воинской части, начиная с роты, должны были предварительно одобряться партийными функционерами.

Однако неразбериха в иерархии командования, созданная этими мерами, подрывала эффективность армии в условиях вторжения американских оккупантов. После войны один из генералов, оставшийся лояльным по отношению к Саддаму, описывал хаос и неспособность к полноценному ведению боевых действий вследствие того, что соседние части и соединения не могли даже контактировать друг с другом: "Это сократило до минимума количество и качество информации, поступавшей из войск, соответственно срывая возможности какого-либо стратегического или тактического планирования". Так как военачальники были поставлены под жёсткий контроль гражданских политиков из БААС, Багдад получал сообщения о ходе боевых действий не от военных, а от политиков. Более того, принятые меры просто-напросто устранили ключевых военачальников и их штабы из цепи командования.

Когда захваченных в плен высших иракских офицеров следователи из ЦРУ просили рассказать о самых главных факторах, приведших к быстрому катастрофическому финалу войны, они отмечали в качестве одной из главных причин "тиранические мероприятия по обеспечению безопасности в армии". Таким образом, ещё до начала войны кибератака США привела к значительному ослаблению структур командования иракскими вооружёнными силами.

Именно против этой ослабленной структуры американцы начали наносить точечные удары с помощью GPS и бомб с лазерным наведением. Авиация США (и сколоченной ими "коалиции") сравняла с землёй в течение короткого времени все госучреждения, известные американцам штабы и бункеры иракской армии, а также квартиры и резиденции ведущих политиков и партийной элиты БААС. Хотя погибло относительно немного функционеров, выбранных в качестве мишени, однако угроза, нависшая над всеми лояльными Саддаму лицами, привела к слому управления войсками.

Для того чтобы избежать гибели от высокоточных американских ракет, иракские политические и военные лидеры избегали совещаний в каких-либо зданиях и бункерах, они перестали пользоваться телефонами и радиосвязью, что оставляло войска без командования, связи и информации о реальном положении дел. После войны иракские генералы горько сетовали на то, что гражданские политики поставили их в практически безвыходное положение. Какие-либо самостоятельные действия на поле боя, предпринятые без согласования с политиками БААС, могли привести к разжалованию и смертному приговору, а слепая неподвижность перед лицом противника неизбежно обрекала их на поражение.

Несомненно, самый большой ущерб от кибератак состоял в том, что Саддам был вынужден предпринимать невероятные усилия для поддержания своей личной безопасности. Он боялся доверять даже самому ближайшему окружению. После начала боевых действий президент скрывался в своих тайных убежищах. Он тщательно следил за тем, чтобы рядом с ним не было людей с телефонами, рациями и другими электронными устройствами.

Из-за всех эти экстраординарных мер военачальники и политики были вынуждены ждать часами, а иногда и днями аудиенции или совещания у главнокомандующего. Учитывая, что они не могли принимать самостоятельные решения, исходя из реальной боевой обстановки, не согласовав их с Саддамом, это также резко снижало боеспособность иракцев. Одним из ярких примеров этого "театра абсурда" было решение о переброске войск, принятое Саддамом на основании полученных ложных сведений. Американцы начали наступление на Багдад с юга 2 апреля, а Саддам получил информацию, что атака готовится с запада. Хусейн приказал генералу Хамдани перебрасывать войска с южного направления. Хамдани точно знал, что наступление будет на его участке, он даже смог убедить в этом сына Саддама Кусея. Однако оба они были не вправе не исполнить полученный приказ, в результате чего южный фронт был оголён. В подобных ситуациях даже не было вины Саддама. Просто в результате принятых мер безопасности разведсообщения с мест приходили со значительным опозданием (иногда на несколько дней), что стало фатальным в условиях быстро развивающегося наступления войск США.

Таким образом, результатом кибервойны США стало полное отсутствие управляемости иракскими войсками. Американские генералы Т. Франкс и Д. Маккирнан отмечали: "Режим не имел никакого представления о том, что реально происходит. Они не знали, где находятся наши войска, они не знали даже, где находятся их собственные войска!"

Саддам Хусейн, лишённый связи, перебирался от одного подземного схрона к другому, пока в городке Ад-Давр, неподалёку от Тикрита, по наводке одного из своих самых доверенных лиц его не захватили 13 декабря 2003 года бойцы элитного отряда "121" во время операции Пентагона и ЦРУ под названием "Красный рассвет". После нескольких лет физических и психологических пыток со стороны американских "спецов" (следы побоев были зафиксированы медиками, приглашёнными адвокатом Хусейна) он прошёл через злобный, издевательский фарс "демократического суда" и был повешен 30 декабря 2006 года. Его сыновья Кусей, Удей и 14-летний внук Мустафа были убиты американцами в июле 2003 года.

Помимо офицеров и генералов, среди "иуд", купленных в ходе кибератак, оказалось очень много государственных чиновников, бизнесменов, членов правящей партии и либеральной интеллигенции, тайно мечтавшей о "свержении тирана" и державшей "кукиш в кармане".

Приближенная к власти творческая элита – артисты, деятели культуры, политологи, ведущие журналисты – получали хорошие барыши, строили виллы в любом районе, который им нравился, получали любые блага и, как они выражались прямо, "продавали себя богатым и влиятельным людям".

Основу действенности американских кибератак представляла всеобщая продажность, которая достигла астрономических размеров. Как известно, проклятие всех "нефтяных" стран состоит в том, что коррупция достигает неимоверных размеров, она становится всеобщей средой, в которой люди проводят ежедневную жизнь.

Создаются синдикаты и сплочённые клики высших чиновников и политиков. Эти шайки, смыкаясь с криминальным миром, включают банки, компании в различных секторах экономики, телевидение и другие СМИ, полицию

и органы безопасности. На законодательном уровне проталкиваются законы, которые позволяли бы коррупционерам беспрепятственно вывозить их капиталы, отмывать их, прятать в офшорах и т. п. Гражданские коррупционеры смыкаются с военными. Аудит общественных организаций не проводится в госучреждениях никогда! А те, кто пытается разобраться в хитросплетениях коррупционеров, подвергаются шантажу, тюремным срокам за несовершённые преступления, избиениям "неизвестными хулиганами", а при особой "настырности" заканчивают свой жизненный путь от руки платных киллеров.

Авторитаризм и "культ вождя" также создавались за счёт опоры на добычу сырья. Нефть оказала сильнейшее воздействие на экономическую политику и позволила Саддаму быть исключительно щедрым по отношению к своим приверженцам, к клике из бизнесменов, военных и правящей партии. Имея в своём распоряжении нефтедоллары, он, как и многие другие лидеры нефтедобывающих стран, строил своё окружение на почитании "вождя", считая себя незаменимым. Это убеждение поддерживалось его окружением, боящимся при смене власти потерять сказочные привилегии и огромные дармовые деньги. Культ личности поддерживался тем, что если выдавались какие-либо награды или денежные поощрения, они выдавались "по приказу президента" или как "подарок от вождя своему народу". Вручали даже особые карточки "Друзья президента и вождя Саддама Хусейна", которые давали их обладателям ряд льгот и преимуществ.

Нефть сформировала экономику Ирака даже в таких далёких от неё сферах, как трудовая миграция и денежные переводы граждан. Но она также привела к колоссальным перекосам в размещении ресурсов, пренебрежению балансом в развитии добывающей и обрабатывающей промышленности, к расширяющейся пропасти между богатыми и бедными. Так было в Ираке, но может быть и в любой другой стране мира.

Во многом благодаря кибертерроризму и деятельности "пятой колонны", Ирак был превращён американцами в руины, погибло огромное количество людей – более 1,5 млн, среди которых 90% составили гражданские лица, включая женщин и детей.

Как же американцы отплатили своим "агентам влияния", иракским предателям?

Большинство генералов и офицеров иракской армии, согласившихся сдать свои позиции и выполнить любые требования США, после капитуляции, потеряв всякую совесть, открыто жаловались в прессе на то, что ЦРУ вообще не заплатило им за предательство, хотя они полностью выполнили приказы своих американских кураторов. Те из них, кто выжили, влачили жалкое нищенское существование.

Оккупационные власти жаловались Вашингтону, что для того, чтобы не было массовых голодных бунтов, им приходится тратить "огромные средства" на содержание бывших военнослужащих иракской армии, "не получая от них никаких услуг взамен". Журналисты подсчитали, что эти "огромные средства" в расчёте на одного человека составляли... 1–2 доллара в день!

Недовольство военных выплеснулось в восстание в Фаллудже. Бывшие офицеры и ополчение 200-тысячного города продержались против атак американцев с апреля по ноябрь 2004 года. Сопротивление удалось подавить лишь после применения запрещённого во всем мире химического оружия – белого фосфора (боеприпасы с ним выжигали всё живое в радиусе 150 м).

Потери среди мирного населения исчислялись десятками тысяч. И последствия американской операции "Ярость Фантома" сказываются до сих пор – уровень онкозаболеваний в городе в 40 раз превышает средний уровень в других местах.

Требовалось срочно решить проблему иракских военных. Именно тогда родилась "отличная" идея – использовать их против правительства Асада в Сирии, очередной мишени Вашингтона в борьбе за мировую гегемонию. Так как правящим кругам США приходилось сталкиваться с возрастающим сопротивлением мирового сообщества и действовать с оглядкой на ООН, наилучшим выходом представлялась война против Сирии руками самих же арабов. Иракских военных (в массе своей суннитов) стали вербовать в ИГИЛ – организацию, созданную якобы для проведения "религиозного джихада" с конечной целью создания "мирового халифата".

В настоящее время даже представители политической элиты Запада (например, экс-министр иностранных дел Великобритании Д. Милибенд, быв-

ший премьер-министр Т. Блэр и др.) признают определяющую роль США в создании, снабжении оружием и военных операциях ИГИЛа.

Таким образом, предателям Ирака нашлась "достойная" роль "пушечного мяса" в кровавых авантюрах Пентагона и ЦРУ на Ближнем и Среднем Востоке. И с ними особо не церемонятся: вчера США вербовали их в ряды ИГИЛ, сегодня кончают их в очередной военно-рекламной операции в Мосуле, направленной на дезинформацию мирового общественного мнения, создания имиджа "непримиримых борцов с терроризмом".

Все государственные компании Ирака были ликвидированы, довоенные контракты (в том числе с Россией и Китаем) аннулированы. Ещё бы, ведь именно из-за нефти и затевалась вся "глобальная война с терроризмом"! Новая конституция Ирака, принятая в 2005 году по указке США, а также другие законодательные акты гарантируют господствующую роль иностранных компаний в добыче нефти. Рокфеллеровский гигант *Exxon* и ротшильдовский *BP* прочно и надолго засели в Ираке и поделили между собой гигантские нефтяные поля этой страны.

А что же либеральная интеллигенция? В отношении этой говорливой и продажной публики американцы ничуть не церемонились. В "стратегии хаоса" предусмотрена ликвидация любой культурной жизни на территории завоёванных "стран-изгоев", низведение их населения до уровня каменного века, сужение культуры лишь до фанатической преданности Аллаху и ненависти к "неверным".

Оккупантами были **разрушены и сожжены библиотеки, учреждения здравоохранения, образования (школы и вузы), культурные центры, уничтожены даже статистические центры, данные переписей населения, рождений и смертей (чтобы нельзя было подсчитать точное количество жертв!)**. Основной удар, безусловно, нанесли по научно-исследовательским центрам и учёным (как гуманитариям, так и представителям фундаментальных и прикладных наук).

А ведь Багдад всегда считался самым престижным центром науки в арабском мире (если говорить об истории, то вся европейская университетская наука была построена по примеру багдадских университетов VIII века).

Фонды и лаборатории были стёрты с лица земли. Спецкоманды рейнджеров из "частных охранных предприятий" (киллеры из *Blackwater* и других "эскадронов смерти") целенаправленно охотились за профессорами, доцентами и научными сотрудниками, убивая их.

После вторжения 2003 года, по данным, опубликованным в египетской прессе (и не оспоренным оккупационными властями Ирака), ежегодно уничтожалось более 300 иракских учёных. Из страны эмигрировали более 20 тысяч преподавателей и научных сотрудников. ЮНЕСКО в 2007 году опубликовала обращение к американцам с просьбой обеспечить безопасность преподавателей и студентов вузов, отметив, что "вся система образования и науки в Ираке находится на грани полного исчезновения". Но отстрелы продолжались и последующие годы. В 2008 году был зверски убит последний иракский нейрохирург, и его растерзанное тело обнаружено на городской свалке...

Не избежали печальной участи и журналисты. Отстреливались все, против кого были даже малейшие подозрения в оппозиционности американцам или стремлении к сохранению традиционных национальных ценностей. Под нож стали попадать и просто "гнилые интеллигенты", которые ранее так стремились слиться в глобалистском порыве с главной "культурной нацией" мира – США. Не уготовано ли это всё и для России?..

– Начинаем кибератаку против России! – это тревожное сообщение поступило из США в октябре 2016 года. И не от какого-нибудь третьеразрядного чиновника, а от вице-президента Дж. Байдена. Это заявление прозвучало весьма угрожающе, ибо из истории последних десятилетий известно, что подобные атаки ЦРУ и Пентагон начинают примерно за год-два до вторжения своих армий на территории "стран-мишеней" либо организации там государственного переворота. В отношении России американцы действуют как напрямую, так и путём организации хакерских групп в Грузии, Латвии, Литве, Эстонии, Польше, Киргизии, Казахстане.

При их "сплочённых действиях" (то есть под руководством КиберКома и спецслужб США), как отмечает известный американский эксперт Р. Андрес, "российские системы безопасности вряд ли смогут справиться с этим мощным наступлением".

Согласно документам *WikiLeaks*, хакеры ЦРУ в настоящее время проводят против России более сотни различных скоординированных кибератак под нарочито "шутливыми" названиями – "Рикки Бобби" (гонщик из комедийного фильма "Ночи Талладеги"), "Бойцовский клуб", "Музыкальный автомат", "Бармен", "Виски", "Маргарита" и др.

"Рикки Бобби", например, представляет собой миниатюрные электронные имплантаты, которые ставятся на новые компьютеры, пользующиеся последними версиями *Microsoft Windows* и *Windows Server*. Они считывают содержание компьютера и не могут быть засечены антивирусными программами и персональными средствами защиты. Эти устройства рассчитаны на автономную работу в течение десяти лет.

Большому риску подвергают страну безрассудные олигархи, использующих в своих проектах западное компьютерное оборудование, которое в определённый момент может привести к сбоям и диверсиям на электростанциях, трубопроводах, системах добычи и переработки полезных ископаемых, транспорте. Не говоря о чисто западных предприятиях автопрома, компьютерной сборки, обрабатывающей промышленности, построенных на российской территории. Российские толстосумы совершают крупнейшую ошибку, вывозя свои миллиарды в офшоры, так как благодаря киберразведке все их электронные счета хорошо известны в ЦРУ и при отказе от сотрудничества будут сразу же заблокированы. (Но и при согласии сотрудничать, как показывает опыт Ирака, эти средства в конечном итоге пополнят счета главных мародёров с Уолл-стрит). Риску подвергают свои жизни те, кто ездит на иностранных элитных авто, летает на американских "Боингах", да и российских самолётах, начинённых западной электроникой. Даже в открытой печати появлялись сообщения о том, что неудачи с запусками ракет были связаны с "ненадёжностью" компьютерных чипов, сделанных по западным лицензиям в азиатских странах. Некоторые крупнейшие аварии и катастрофы последних месяцев вполне укладываются в рамки классического кибертерроризма.

Как и в отношении Ирака, кибертерроризм США, нацеленный против России, сочетается с кампанией шантажа и угроз. И, складывается впечатление, что на первом этапе их "мишенями" стали опытные российские дипломаты, обладающие мощным влиянием на политическую элиту и общественное мнения стран, где они представляют интересы России.

Многие международные эксперты обратили внимание на "странные смерти" российских послов в декабре 2016 – январе 2017 годов Один из них пишет: "Мы не провидцы, не разведчики, мы лишь политические аналитики. Но уже в конце прошлого года мы пришли к выводу, что Запад будет организовывать убийства или компрометацию российских послов. В рамках этой кампании смерть российского представителя в ООН В. Чуркина выглядит вполне логичной. Да и диагноз "неожиданного сердечного приступа" в последнее время ставится довольно часто в качестве причины смерти неугодных "мировой закулисе" политиков. Известно, что эти "приступы" могут вызываться многими искусственными причинами, и в открытом доступе есть достаточно материалов о таких средствах, которые вызывают остановку сердца, и их практически невозможно идентифицировать после смерти намеченной жертвы".

В. И. Чуркин, российский представитель в ООН, яркий политик, открыто выступавший с трибуны ООН против американского и израильского империализма, "неожиданно" умер на своём рабочем месте 20 февраля 2017 года. У него были широкие связи и контакты с политиками США и других стран, придерживавшимися антиимпериалистических взглядов.

А до него 19 декабря 2016 года во время открытия выставки был публично убит сотрудником турецкой спецслужбы российский посол в Турции А. Г. Карлов. Чудом выжил после "пищевого отравления" в конце декабря 2016 года посол РФ в Израиле А. П. Шеин. Странной была смерть в январе 2017 года посла России в Индии, опытнейшего и авторитетного специалиста А. М. Кадакина. В том же январе "неожиданно" в Греции, в своей квартире в центре Афин скончался 55-летний российский дипломат, консул Андрей Маланин.

Наряду с этими смертями идёт и прямое запугивание тех, кто, видимо, не склонен сотрудничать с западными спецслужбами. Так, 14 января в СМИ прошло сообщение о том, что в результате теракта были убиты посол РФ в Йемене А. П. Дедушкин и ещё два сотрудника посольства. МИД РФ опровергло эту информацию. Однако ряд экспертов считают, что эта "деза" была организована

британской разведкой с помощью саудовских новостных агентств как "психологическая атака" на российский МИД.

Стратегия государственного кибертерроризма США включает в себя обострение информационной войны, оголтелую пропаганду и всемерное нагнетание военной напряжённости.

Нынешнее противоборство между Трампом и сторонниками Х. Клинтон многие российские эксперты ошибочно трактуют как столкновение между "ястребами" и "голубями". На самом деле сторонники Трампа (включая небезызвестного Г. Киссинджера) отнюдь не выступают за "мир и дружбу", они просто пытаются использовать против России методы "мягкого удушения", которые оказались весьма действенными в преддверии развала СССР. Их же противники не желают никаких "послаблений", они уверены в том, что **Россию надо просто стереть с лица земли имеющимися у США военными средствами**.

И их точка зрения, растиражированная практически всеми американскими СМИ, фактически поставила на колени администрацию Трампа! Он был вынужден уволить советника национальной безопасности генерала М. Флинна только за то, что тот разговаривал по телефону с российским послом в США С. И. Кисляком и неофициально просил не принимать меры в ответ на беспрецедентную высылку из США 35 российских дипломатов, инициированную администрацией Обамы в декабре 2017 года. Этот разговор сыграл свою роль в отказе российской стороны применить обычные в подобных случаях "симметричные шаги". Но вместо благодарности за смягчение напряжённости в отношениях между США и Россией пресса и спецслужбы обвинили Флинна – ни много ни мало – в государственной измене!

Мало того, что ЦРУ использовало против Флинна методы кибертеррора, поставив прослушку и записав разговоры частного лица (тогда генерал ещё официально не был членом президентской администрации), но для возбуждения уголовного дела из пыльных архивов вытащили на свет так называемый "закон Логана", принятый в 1799 году. Он запрещал несанкционированные контакты частных лиц с государственными деятелями зарубежных стран, и поводом для него стали переговоры Дж. Логана с французскими властями в период, когда централизованная государственная власть ещё не укрепилась в США после войны за независимость. Закон за всю историю страны **ни разу не использовался (!)**, в том числе против самого Логана, который уже после его принятия не побоялся вести частные переговоры с англичанами в 1810 году. И вот теперь этот мертворождённый документ использовали, чтобы обвинить Флинна в "тяжком преступлении".

Это говорит о безумном градусе паранойи, нагнетаемой в прессе, на ТВ, в выступлениях американских политиков. Известный политолог П. К. Робертс пишет: "Русских демонизируют и приписывают им поистине демонические силы. Если вы заговорите с русским (или даже просто о России), вы сразу же подпадаете под подозрение в государственной измене. На вас сразу же обратят недреманное око ЦРУ, Демократическая партия, ВПК и проститутки из СМИ. Как только Трамп принёс в жертву своего советника по национальной безопасности, он подставил под огонь не только всех остальных членов своей администрации, но и самого себя. Он следующий на очереди".

Генерал Маттис, нынешний глава Пентагона, назначенный Трампом, перешёл к обычному за последние годы лицемерному осуждению "агрессивности" России: "Начиная с Ялты (имеются в виду Ялтинские соглашения 1945 года. – **Н. И.**), мы в течение долгого времени пытались наладить отношения с Россией, но в целом безуспешно".

Эта фальшивка о "добрых намерениях" США и "несговорчивости русских" повторяется в СМИ неустанно, год за годом и служит прикрытием для стягивания войск и ракет к границам РФ. Только в январе этого года США разместили вблизи от российской границы самые большие военные силы за последние четверть века – в январе в Польшу, Румынию, Болгарию, Германию, Венгрию и страны Балтики было переброшено около 4 тысяч военнослужащих США, большое количество оружия и снаряжения, 2500 танков, грузовики, БТРы. Ф. Ходжес, командующий американскими войсками в Европе, заявил: "Прошли годы после того, как последние американские танки были вывезены из Европы, и вот настало время для их переброски в обратном направлении".

Эти меры, утверждает генерал Ходжес, были предприняты в ответ на "агрессию России на Украине и незаконную аннексию Крыма, и они не означают

автоматически, что война неизбежна, – всё будет зависеть от позиции Москвы". Что это, если не очевидный военный шантаж и сигнал к активизации в России "пятой колонны"?!

Есть ли возможности для отпора кибертерроризму (а возможно, и открытому военному противостоянию)? Конечно, многие скажут, что можно создать технические средства, которые бы заблокировали кибератаки, наладить производство своих компьютеров, "софта", электронных чипов, мобильных телефонов, телевизоров и прочих "гаджетов" (хотя даже это требует экстраординарных усилий, энергии и воли чиновников, концентрации финансовых средств, огромных капиталовложений в российскую экономику, а не в офшорные счета на Каймановых островах).

Но как решить основную задачу – избавиться от предательской "пятой колонны"? Ведь можно подкупать и шантажировать чиновников, военных, журналистов не только через интернет, но и открытые каналы и прямые контакты. В разгар кибератак против Ирака в начале 2000-х годов многие честные и патриотически настроенные иракские эксперты давали Саддаму советы, которые были очевидными для всех.

Прежде всего, надо было установить полный контроль над финансами страны. Отменить порочную привязку к доллару. Минимизировать и свести на нет иностранные инвестиции и кредиты (доходы от них идут твоему противнику – США, а не в бюджет Ирака, их используют для подкормки "пятой колонны", максимального ослабления национальной валюты и организации биржевых крахов). Взять под полный контроль Центробанк и выгнать оттуда "поганой метлой" либеральных "монетаристов" и "рыночников", подрывающих национальную валюту. Увеличить эмиссию денежных средств и обеспечить кредитами экономику, которая заработает полноценно.

Взять под полный контроль филиалы транснациональных корпораций, которые во всех войнах и госпереворотах играют решающую роль в создании обстановки саботажа, сборе ценнейших разведданных, прикрытии работы спецагентов и диверсионных команд (достаточно вспомнить деструктивную роль *ITT*, "Макдональдса", "Кока-Колы" и других американских компаний в свержении правительства Альенде в Чили в 1973 году, в недавних событиях в Бразилии и Венесуэле).

Снизить зависимость правительства от нефтяных и прочих олигархов, ориентированных на Запад, переводящих туда миллиарды долларов. Отказаться от порочной тактики приватизаций и сосредоточить главные экономические рычаги в руках государства. Бросить все силы и средства на развитие "оборонки". Максимально диверсифицировать экономику.

Ускорить процессы импортозамещения. Снизить зависимость власти от либерально-монетаристских экономистов и политиков. Искать опору не среди "эффективных менеджеров", а среди честных технократов, не рантье, а предпринимателей, не спекулянтов, а производителей. Иными словами, надо перейти к национальному, общественному и производительному характеру развития экономики.

В сфере культуры надо было бороться против пустых, бессодержательных и вредных голливудских фильмов, против "американизации" молодёжи. Ведь она составляет обширную "матрицу", на которой произрастают антинациональные, предательские настроения. Бороться за чистоту языка, убирать американские вывески и рекламу, иностранщину в речи и журнальных статьях.

Главная задача – "революция в головах" людей. Необходимо было изменить ценностную ориентацию общества. Вместо потребительства, гедонизма, эгоизма, развлечений, получения максимального удовольствия целенаправленно воспитывать культ долга, ответственности, служения Родине, товарищества, коллективизма, взаимовыручки, творческого труда.

Но Хусейн (прежде всего, под влиянием угодливых "придворных") не прислушался к мудрым советам. А ведь можно было создать из иракского общества монолит, о который американцы со своим кибертерроризмом обломали бы зубы. Да и открытая война пошла бы по совершенно иному сценарию. Ведь даже самые оголтелые "ястребы" из Пентагона подсчитали, что если потери американцев в первые недели боевых действий превысят 20 тысяч человек, то придётся бесславно заканчивать операцию из-за роста недовольства внутри США. И, глядишь, "Шок и трепет" постиг бы не иракцев, а самих американцев, и не помогли бы им никакие, самые изощрённые "кибератаки".

Руководству России надо задуматься над всем этим.