

ТИМ ДЖОРДАН

КИБЕР- ГЕРИЛЬЯ

ЦИФРОВОЕ
ПОДПОЛЬЕ
ПРОТИВ
ПЕНТАГОНА



Тим Джордан
Кибергерилья. Цифровое
подполье против Пентагона
Серия «Против течения»

Текст предоставлен правообладателем

http://www.litres.ru/pages/biblio_book/?art=74611476

*Кибергерилья. Цифровое подполье против Пентагона: Родина; Москва;
2026*

ISBN 978-5-00269-336-8

Аннотация

В конце восьмидесятых годов компьютеры постепенно перестают быть уделом исследовательских лабораторий и начинают массово применяться американским государством для укрепления своей власти. Активно идет оцифровка полицейских баз данных, документооборота Пентагона и НАСА, компьютеры внедряются в ЦРУ.

Именно тогда появляется новая, невиданная доселе угроза – хакеры. Они взламывают еще примитивные компьютерные сети полиции, армии и спецслужб Америки, уничтожают информацию, публикуют секретные документы. Поймать их оказалось невозможно. Постепенно старая городская герилья, знакомая нам по семидесятым, уходит в прошлое. Ее место занимает герилья в киберпространстве, где действуют

хакеры, социальные инженеры, активисты, борцы за свободу информации.

Эта книга рассказывает о первых хакерских группах и истории их возникновения, об их целях и об идеях, которые их вдохновляли.

В формате PDF A4 сохранен издательский макет книги.

Содержание

Глава 1. Взлом и хактивизм	6
Конец ознакомительного фрагмента.	33

Тим Джордан

Кибергерилья. Цифровое

подполье против Пентагона

© Джордан Т., 2026

© Катайцева Э. С., перевод, 2026

© Нигматулин М. В., перевод, 2026

© ООО «Издательство Родина», 2026

Глава 1. Взлом и хактивизм

Протест, ставший электронным

Наличие массового политического протеста – характерная черта любого сообщества; он может проявляться в ярких уличных демонстрациях или в не слишком заметных собраниях местных объединений. Самоорганизация людей свидетельствует об их желании влиять на пространства и время своей жизни, даже пытаться контролировать их, пусть и в условиях, не выбранных ими. Это желание и сопутствующие ему ограничения проявились и в пространствах виртуальной жизни – как в попытках контролировать киберпространство, так и в действиях, направленных на влияние в офлайне через киберпространство.

Хактивизм – это возникновение массового политического действия, самоорганизации групп людей в киберпространстве. Это сочетание низовой политической акции с компьютерным взломом. Хактивисты действуют в ткани киберпространства, споря о том, что технологически возможно в виртуальной жизни, и выходят за его рамки, используя виртуальные возможности для преобразования офлайн-реальности. Социальные движения и массовый протест – неотъем-

лемая часть общества XXI века. Хактивизм – это активизм, ставший электронным.

Хотя движения в защиту киберпространства существуют уже некоторое время, появление массового протеста внутри киберпространства – будь то протесты о самом киберпространстве или с использованием киберпространства – относительно новое явление. Эта книга посвящена возникновению виртуальных прямых действий. Хактивизм не означает любую политику, связанную с киберпространством – тогда вся политика стала бы хактивизмом, потому что сейчас очень немногие области социального и культурного конфликта не затрагивают виртуальность в той или иной форме. Скорее хактивизм, возникший в конце XX века, – это конкретное социально-культурное явление, в котором массовая политика прямого действия была перенесена в виртуальные сферы. Это не исключает существования других форм массовой или движенческой политики в киберпространстве; просто здесь мы сосредотачиваемся на определённом типе киберполитики. Как выразилась одна из пионерских групп хактивистов:

– Правила культурного и политического сопротивления радикально изменились. Революция в технологиях, вызванная быстрым развитием компьютеров и видео, создала новую географию соотношения сил в странах «первого мира», которую ещё двадцать лет назад можно было лишь представить: люди сведены к данным, наблюдение осуществляется

в глобальном масштабе, умы сливаются с экранной реальностью, и возникает авторитарная власть, процветающая на основе отсутствия. Новая география – виртуальная география, и суть политического и культурного сопротивления должна заявить о себе в этом электронном пространстве.

Эта книга картирует один из ключевых компонентов новой географии власти: онлайн-прямые действия, или хактивизм. Чтобы первоначально прояснить хактивизм, нам нужно выделить ряд вопросов. Его внезапное и порой шокирующее появление стало результатом пересечения трёх различных течений: взлома, информационных обществ и современного социального протеста и сопротивления. Ниже приводится структура книги и содержание, показывающие, как мы отслеживаем эти три направления, чтобы поместить хактивизм в соответствующий политико-культурный контекст и сделать яснее и его новизну, и его корни. После того как будут обозначены основные влияния хактивизма, станет возможным очертить его ключевые компоненты и последствия.

Взлом

Изначально взлом основывался на творческом переосмыслении потенциала технологий в контркультурных и оппозиционных сообществах. Однако к середине 1990-х годов технологическая экспертиза взлома, с одной стороны, всё больше приспособлялась к коммерческому менталите-

ту развивавшихся интернет-индустрий, а с другой – всё больше ассоциировалась с незаконным компьютерным проникновением. Учитывая дискуссии о терминологии и точных временных рамках, хактивизм зародился примерно в этот период, возможно, совпав с самым низким моментом в истории первичного контркультурного статуса взлома.

К середине 1990-х стало труднее воспринимать взлом как контркультурное или подпольное явление: революция интернета и персональных компьютеров сначала охватила развитые страны, а затем мир в всё более коммерческом формате. Расширяющиеся компьютерные компании нанимали тысячи специалистов, фактически создавая и поглощая тех людей с компьютерной подготовкой, которые раньше встречались преимущественно в субкультурах взлома. Взлом и хакеры стали частью многомиллионных бизнесов; пришли «микросерфы». Одновременно в массовом восприятии к взлому прочно прикрепилась негативная ассоциация с вредоносным компьютерным проникновением. В медиа «хакер» стали понимать как того, кто незаконно или злонамеренно получает доступ к чужому компьютеру. Появлялись истории о взломе почтовых ящиков, похищении данных кредитных карт и банковских ограблениях, совершённых исключительно электронными средствами. Взлом стал синонимом использования технических навыков для совершения компьютерной преступной деятельности. Именно в этот момент истории взлома зародился хактивизм.

Чтобы полно понять этот момент, сначала кратко опишем, что такое «хак», а затем представим шесть широких стадий, через которые прошёл взлом до появления того, что мы назовём седьмым поколением: хактивисты. Эти описания не претендуют на исчерпывающий характер, а служат для того, чтобы полностью обозначить как корни хактивизма во взломе, так и его ключевые отличия.



Джулиан Ассанж.

Базовый элемент культуры взлома – unsurprisingly – «хак», и, опять же, чтобы понять хактивизм, полезно ознакомиться

с этим понятием. Хак когда-то и до сих пор в определённых кругах означает блестящую программную уловку. Несмотря на коннотации незаконных вторжений, внутри хакерских кругов хак чаще определяется как попытка использовать технологию оригинальным, неортодоксальным и изобретательным способом. Главный спор, порождённый криминальными формами взлома, заключается в том, насколько изобретательность хакерской техники должна подчиняться её легальности. Хотя это вечные дебаты, здесь хак представлен в самом широком смысле, чтобы оценить возможное сходство между его незаконными, озорными и законно гениальными формами.

Исследователь предложила концептуализацию основных элементов взлома, подтверждённую более поздними качественными исследованиями. Она объединяет более широкое определение незаконного взлома с общей ментальностью тех, кто видит взлом как манипуляцию любой технологией для неортодоксальных целей. Она описывала хак как «Святой Грааль»: концепт, существующий независимо от компьютера, и его лучше всего проиллюстрировать на примере другой технологии, достаточно сложной, чтобы поддерживать собственную версию хаков и хакеров. В качестве примера приводился взлом телефонных систем, и один из его пионеров, Джон Дрейпер, известный как «Капитан Кранч». Хак в этом случае – это такие технологические трюки, как поставить два телефона на стол, говорить в один и через некоторое

время услышать свой голос в другом, после задержки, когда исходный вызов был маршрутизирован вокруг света. Всё это делалось незаконно и без оплаты телефонным компаниям. Эта исследовательница понимала такой хак следующим образом: ценность звонка, прошедшего вокруг света, – упражнение в эстетике хакера. Это напроць удивительный результат, достигнутый невероятно простыми средствами. Важно также то, что Дрейпер не просто наткнулся на любопытство; трюк работал потому, что он приобрёл впечатляющую экспертизу о телефонной системе. Именно это делало трюк великим хаком; в противном случае это был бы лишь незначительный фокус. Мастерство является сутью культуры хакеров. Кроме того, экспертность приобреталась неофициально и за счёт большой системы. Хакер – человек вне системы, который никогда не исключён её правилами.

Основные характеристики хака – простота, мастерство и незаконность. Важно отметить, что ключевой аспект данного анализа заключается в том, что суть хака заключается в эклектичном прагматизме, с которым хакеры подходят к любой технологии. В этом смысле взлом традиционно ассоциировался с такими разнородными занятиями, как отмычки и обслуживание модельных железных дорог (и с сопутствующей вознёй с гаджетами). Сами хакеры указывают на широкий спектр своих возможных целей:

– В моей повседневной жизни я взламываю всё, что только можно представить. Я лажу со светофорами, уличными

будками, автоответчиками, микроволновками, видеомагнитофонами – не вспоминая и не задумываясь. Для меня хак – это просто постоянное изменение условий до тех пор, пока не появится другой отклик. В сегодняшнем механическом мире возможностей для такого экспериментирования предостаточно.

Разнообразие технологических объектов, считающихся «взламываемыми», описывает нидерландский хакер Р., который утверждал, что понятие «взлом» должно охватывать не только компьютеры, но и любую область технологии. По его словам, «если у тебя нет чайника, чтобы вскипятить воду, и ты используешь для этого кофемашину, – это взлом». Потому что ты используешь технологию не по её прямому назначению. То же самое относится к телефонам: если ты применяешь телефон для задач, не предусмотренных его создателями, это тоже взлом. Если ты автомеханик и заставляешь двигатель делать то, для чего он не предназначен, это взлом. Таким образом, взлом – это не только компьютеры, а всё, от замков и телефонов до магнитных карт.

Три элемента – мастерство, простота и элемент запретного – создают особое чувство азарта, «кайф» от взлома. Разнообразие целей взлома усиливает это ощущение, подпитывая технологическое любопытство. В первые годы освоения электричества, когда люди вроде Теслы проводили эксперименты, они, по сути, были хакерами своего времени – исследователями границ технологии, движимыми не только нау-

кой, но и удовольствием от самого процесса.

Этот «кайф» напрямую связан с изобретательностью, которая отличает подлинные взломы от тех, что можно назвать проявлением упорства без креативности – когда преобладают усердие и настойчивость, но не оригинальность. Существует также различие между оригинальными взломами и заранее подготовленными атаками. Последние могут быть запущены, но не придуманы людьми, которых презрительно называют «дети-скрипты». Способы взлома часто становятся достоянием общественности через журналы, хакерские конференции или просто электронное общение. Из таких источников возникают «кулинарные книги» с готовыми инструкциями. Те, кто использует такие методы, не внося ничего нового, считаются хакерами лишь в том смысле, что занимаются несанкционированным использованием технологии. Настоящие хакеры стараются отграничить себя от таких людей, утверждая, что их деятельность связана с творчеством и экспериментом.

Пример телефонного фрикинга хорошо иллюстрирует это различие. Если кто-то изучает устройство телефонной будки, понимает, что, перерезав провод, можно обойти систему, и экспериментирует с этим, – это хакер. Но если другой человек просто читает об этом, повторяет трюк ради бесплатного звонка и ничего не создает – он дилетант. А вот тот, кто, узнав об идее, развивает её, например, добавляя магнитный переключатель, чтобы можно было временно разь-

единять провода и затем возвращать их в исходное состояние, проявляет настоящее хакерское мышление. Это не чёрно-белое различие, но оно показывает суть.

Взлом – это действие, которое хакеры совершают или считают, что совершают. Это простейшее определение взлома и одновременно идеал. Как и все люди, хакеры не всегда соответствуют собственному идеалу, поэтому вокруг взлома возникли сообщества с собственной культурой и символикой. Поняв, что представляет собой суть взлома, можно рассмотреть, как это проявлялось в истории хакерского движения. Взлом существует только в действии, совершаемом хакерами, а сами хакеры существуют внутри сообщества. Чтобы понять, что отличает их от других, нужно рассмотреть, как их представления о себе выражаются в коллективных отношениях. Эти сообщества претерпели значительные изменения, и можно выделить шесть различных, хотя и пересекающихся, групп, объединённых общей преданностью идее взлома. Эти сообщества обозначают исторические этапы развития хакерства и стали предшественниками хактивизма – использования взлома для политических целей.

Развитие хакерского сообщества во времени и пространстве

Трудно разложить развитие хакерства по чётким хронологическим периодам. Схема семи поколений хакеров даёт

лишь приблизительное представление об изменениях, произошедших в компьютерном подполье. Она не отражает пересечений во времени и различий в этических принципах: представители всех поколений нередко утверждают, что разделяют дух первой волны. Кроме того, само определение того, что считать взломом, вызывает споры как внутри, так и вне сообщества, и границы между «хорошим» и «плохим» взломом, а также между хакерством и хактивизмом остаются размытыми.

Первые исследователи хакеров выделяли три пересекающиеся группы, применявшие понятие «хорошего взлома» к разным видам технологий:

«Оригинальные» хакеры – первопроходцы компьютерного дела, работавшие с большими ЭВМ в университетах США в 1950–1960-х годах.

Хакеры «железа» – новаторы, сыгравшие ключевую роль в революции персональных компьютеров 1970-х, сделавших вычислительную технику массовой и децентрализованной.

Хакеры «программного обеспечения» – специалисты, создававшие или модифицировавшие программы для новых компьютеров, нередко разработанных их друзьями из числа «железных» хакеров.

Эти три сообщества, сформировавшиеся с конца 1960-х до середины 1970-х, тесно переплетались, и многие люди могли относиться сразу к нескольким. Из их взаимодействия выросло общее хакерское движение, сосредоточенное

на идеальном взломе.

Позже появились новые поколения и подсообщества. Их нельзя рассматривать как отдельные, изолированные группы – это пересекающиеся сети хакеров, среди которых многие одновременно принадлежат к нескольким направлениям. Первые три категории можно считать «первым поколением» хакеров, за которыми почти сразу последовала «вторая волна».

Во второй волне хакеры стали восприниматься как субкультура. Они начали привлекать внимание СМИ, поскольку выглядели уверенно в мире новых технологий, тогда как общество испытывало страх и растерянность перед информационной революцией. Например, организация Electronic Frontier Foundation защищала хакеров, считая их действия вопросом гражданских свобод, и выступала против антицифрового консерватизма, угрожавшего общественному развитию. Хакеры стали восприниматься как жители переходного пространства между старым обществом и новой технологической эпохой.

Хакерство рассматривалось как постмодернистская контркультура – ироничная реакция на власть технологий, подрыв устоявшихся норм, игра с границами допустимого. Хакеры выражали сопротивление не самой технологии, а её доминированию, бюрократии, контролю и утрате личного пространства.

Возвышенный статус, который хакеры получили в глазах

общества, в значительной степени связан с хакерами «железа» и «программ», чьи разработки впервые напрямую затронули повседневную жизнь людей. Дальнейшее развитие хакерства можно описать через четыре взаимосвязанные и пересекающиеся группы.

Хакер и крэкер: с середины 1980-х годов оба эти термина используются для обозначения человека, который незаконно проникает в чужие компьютерные системы, хотя не всегда из злых побуждений. Выбор слова зависит от точки зрения говорящего. Слово «хакер» чаще употребляется людьми вне компьютерного подполья, особенно в СМИ. Слово «крэкер» предпочитают использовать в технических кругах – как среди подпольных хакеров, так и в легальной сфере кибербезопасности, – чтобы сохранить за термином «хакер» более благородный смысл изобретательного обращения с любой технологией.

Микросерфы: в романе Дугласа Коупленда *Microserfs* этот термин описывает программистов, которые, сохраняя черты хакерской субкультуры, всё же оказались поглощены структурами крупных корпораций вроде Microsoft. Несмотря на своё техническое мастерство и независимый дух, они стали частью корпоративного класса, владеющего акциями, – своеобразным электронным средним сословием.

Открытый исходный код: стремление создавать лучшее программное обеспечение привело к появлению сообщества, которое открыто публикует свои разработки, чтобы

другие могли их улучшать. Это сообщество противопоставляло идею свободных и изящных решений громоздким коммерческим продуктам и тем самым создало основу для появления бесплатного и постоянно совершенствуемого программного обеспечения. Появление Linux как серьёзного конкурента Windows стало символом становления этого движения как влиятельной силы в мире технологий.

Хактивисты: в середине 1990-х годов хакерская деятельность соединилась с открытой политической позицией.

Таким образом, хакерское сообщество включает семь различных поколений или групп, за исключением, пожалуй, первых хакеров, чьи мейнфреймы остались в прошлом. Сегодня всё ещё существуют хакеры «железа» и «программ», а микросерфы, крэкеры и движение открытого кода прочно закрепились. Чтобы понять связь между хакерством и политикой – именно она отличает хактивизм от других форм инновационного использования технологий, – необходимо рассмотреть природу самого хакерского сообщества. Начать можно с анализа политических взглядов первых двух поколений хакеров.

Ранняя хакерская политика

Это были радикальные, почти партизанские хакеры, которые сумели придать компьютеру совершенно новый образ и политическое измерение, недостижимое для крупных

корпораций вроде IBM и их последователей. Благодаря им информационные технологии приблизились к тому, чтобы стать инструментом демократической политики.

В эпоху «электронного популизма» хакеры стали не только техническими первопроходцами, но и вдохновляющими фигурами. Рассмотрение политизированных аспектов раннего хакерства помогает понять, как внутренние ценности движения привели к возникновению хактивизма. Среди хакеров первого поколения были те, кто имел радикальные политические взгляды и стремился сделать вычислительную мощность доступной для всех. Однако на практике их цели часто размывались из-за более насущной задачи – получить доступ к сложным системам, соответствующим их техническому уровню.

Этика ранних хакеров основывалась на идее неограниченного доступа к вычислительным мощностям и информации. Для многих стремление к взлому и желание сделать технологии демократичными и доступными были двумя сторонами одной медали. Но это стремление имело двойственную природу: с одной стороны, оно способствовало прогрессивным, даже утопическим идеям о свободном обществе, а с другой – нередко отдаляло хакеров от социальных проблем, погружая их в мир технологий.

Первые проявления социально радикальных импульсов можно увидеть в деятельности группы Йиппи. В 1971 году Эбби Хоффман участвовал в создании подпольной газе-

ты Youth International Party Line (YIPL), выступавшей против решения правительства США финансировать войну во Вьетнаме через налог на телефонные счета. Газета призывала отказываться от уплаты этого налога как формы протеста против войны. Позже издание стало технически ориентированным и в 1973 году сменило название на Technological American Party (TAP). В его выпусках публиковались подробные инструкции по телефонному фрикингу – получению бесплатных звонков путём манипуляций с телефонной системой, а также материалы о радиопиратстве, отмычках и обходе счётчиков.

TAP прекратил существование в 1984 году, но его идею продолжил журнал 2600, посвящённый фрикингу и хакерству. В Европе примерно в то же время появился немецкий Chaos Computer Club (CCC), который выдвинул лозунг «Вся информация хочет быть свободной» и отстаивал право на свободную коммуникацию и обмен знаниями по всему миру.

Антикорпоративные настроения, характерные для первых хакеров, сохранились и во втором поколении, что отражалось даже в названиях небольших компаний вроде Itty-Bitty Machine Company (пародия на IBM) и Kentucky Fried Computers. Однако этот дух свободы вскоре уступил место коммерциализации. Компьютеры, некогда символизировавшие освобождение, превратились в потребительские товары. Яркие перспективы, открывавшиеся новыми технологиями, оказались удивительно совместимы с корпоративным

контролем и коммерческой выгодой. Информация стала товаром, а компьютерная индустрия – мощным инструментом капитализма. Надежды на использование компьютеров как средства противостояния власти растворились в электронных развлечениях и жажде прибыли.

Со временем политический заряд хакерства ослаб. Изначальное стремление расширить демократию через свободный доступ к информации сменилось более эгоистичными мотивами – жадой доступа к технике ради самой техники и стремлением к коммерческому успеху. Антиавторитарные настроения стали восприниматься не как форма протеста, а как проявление неудовлетворённого потребительского инстинкта – желания пользоваться ресурсами, которые недоступны для «покупки».

Такое разочарованное восприятие выразилось в романе Дугласа Коупленда *Microserfs*, где он описывает жизнь молодых программистов, работающих в штаб-квартире Microsoft. Здесь впервые показано полное слияние корпоративного и личного пространства. Компания предоставляла работникам душевые, зоны отдыха и всё необходимое, чтобы человек фактически жил на работе. В 1990-х этот процесс зашёл так далеко, что корпорации перестали нанимать людей – люди сами становились корпорациями.



Штаб-квартира агентства DARPA.

Появление микросерфов как отдельной группы хакеров наряду с крэкерами обозначило политический спад хакерской культуры. Корпорации вроде Microsoft сумели ассимилировать хакерские черты – страсть к программированию, увлечение кодом – и обратить их на службу «силиконовому капитализму».

В ответ на это в 1990-х возникли два новых направления – движение открытого кода и хактивизм. Они символизировали возвращение к изначальным антикоммерческим и контр-

культурным ценностям хакерства, стремление противостоять превращению технологий и человеческой жизни в товар.

Движение за открытое программное обеспечение всё больше утверждало себя, возвращая изначальный смысл понятию «хак», и происходило это в условиях гиперкоммерциализированного бумаинтернета, предшествовавшего краху доткомов. Хотя движение открытого исходного кода является сложным явлением, в его основе лежит стремление создавать изящные программы путём обмена исходным кодом внутри сообщества, которое может проверять и улучшать любые решения. Процесс заключается в том, что кто-то создает программный код и выкладывает его, чтобы другие могли его критиковать, совершенствовать и развивать. Почти всё такое программное обеспечение распространяется бесплатно, с единственными ограничениями – его нельзя продавать, а любые улучшения должны быть доступны другим для изучения и дальнейшего совершенствования. Известная операционная система Linux, широко используемое программное обеспечение веб-сервера Apache и развитие браузеров Netscape в проекте Mozilla – всё это, в той или иной форме, примеры проектов с открытым исходным кодом.

Хотя само движение и его сторонники существовали уже много лет, возможно, являясь прямыми наследниками первого поколения хакеров, долгое время оно оставалось делом лишь технически одарённых людей. Преданность идее

создания элегантного программного кода часто изолировала участников движения от широкой публики, которая не могла использовать или понять их труд.

Это постепенно начало меняться в 1990-х и в начале XXI века, когда различные проекты открытого исходного кода оживили хакерское сообщество и придали ему значение, которое раньше казалось невозможным. Особенно заметное влияние оказала растущая популярность Linux, которая помогла вернуть слову «хакер» его первоначальный высокий смысл. Хотя нет возможности подробно пересказать историю движения, важно отметить его растущую известность и силу, а также радикальную приверженность идеям свободы информации и сопротивлению коммерциализации программного обеспечения – всё это происходило параллельно с возникновением хактивизма. В этом смысле открытое программное обеспечение – политически заряженное движение, сосредоточенное на свободе информации, хотя его политическая сущность часто остаётся скрытой в строках кода. В то же время появлялась группа хакеров, чьи политические мотивы невозможно было игнорировать или спрятать в программном обеспечении. Именно использование компьютеров как инструмента прямого действия и сформировало хактивизм как особое сообщество в мире хакеров.

Прямое действие и хактивизм

С ростом роли компьютеров и учитывая, что наши политические противники – одни из самых технологически оснащённых людей в мире, было бы глупо игнорировать компьютер. Напротив, необходимо обратить на него внимание, понять его и превратить в инструмент сопротивления. Для тех, кто сопротивляется компьютерам, стоит задуматься об использовании компьютеров для сопротивления.

Хактивизм имеет свои корни в бурных потоках хакерской культуры. Уже более полувека технари – как внутри, так и вне официальных институтов – экспериментируют с компьютерными технологиями, стремясь к моментам мастерства, простоты и дерзости. Через два поколения хакерства – от корпоративного присвоения идей до подпольной одержимости взломами – хактивизм, наряду с движением открытого исходного кода, сформировал хактивистское сообщество, которому посвящено данное исследование.

Однако прежде чем рассматривать конкретные формы прямых действий, необходимо очертить два контекста. Первый – это общесоциальный и культурный фон новой информационной или сетевой эпохи. Второй – это история массовых протестов и прямых действий, неожиданно переплетенная с хакерством в феномене хактивизма. После описания этих предпосылок исследование сосредоточится на двух ос-

новых типах прямых действий хактивистов: массовых акциях и цифровых акциях точечного воздействия. Завершат анализ размышления о социальном и теоретическом значении хактивизма.

Почти полная зависимость современных государств и глобального капитализма от сложных коммуникационных сетей создала условия для появления новой политической повестки, добавленной к существовавшим в хакерской культуре антисистемным, но антиавторитарным тенденциям. Стремительный рост числа таких сетей одновременно усилил процессы глобальной коммерциализации и повысил их уязвимость перед силами несогласия. Хактивизм вырос из хакерства как угроза коммерциализации и государственному контролю над информацией.

Вирусное время

Последствия успешного супервируса трудно даже представить. По словам одного эксперта по компьютерной безопасности из Лондона, «это было бы так, словно эффект “ошибки 2000 года” действительно осуществился». Источники, близкие к британским спецслужбам, утверждали, что некоторые террористические организации рассматривали возможность атак на системы управления воздушным движением с помощью вирусов или взломов. Прогнозировалось, что подобные действия могут быть приурочены к акциям

протеста против международных финансовых институтов, чтобы усложнить расследование. Некоторые группы, связанные с анархистскими движениями, включали в свои ряды хакеров.

Конец XX века стал моментом осознания того, что природа общества изменилась. Возникли новые социальные и культурные формы, которые описывались как информационные, постиндустриальные, постмодернистские, мобильные или сетевые. Вместо споров о том, является ли это чем-то принципиально новым, внимание сосредоточилось на анализе этих форм. Именно в этих новых реалиях и возник хактивизм – политика, основанная на информации и существующая в информационную эпоху.

Следует подчеркнуть, что это не экономическая «база», которая объясняет хактивизм, а комплекс социальных, культурных, политических и экономических тенденций, в которых он укоренён и которые, в свою очередь, он формирует.

Как и все новые формы, информационное общество не уничтожает полностью старые модели. Так же как феодальные структуры сохранялись внутри индустриального капитализма, изменяясь, но продолжая существовать, так и в информационную эпоху старое и новое сосуществуют. Стремление к прибыли через эксплуатацию труда, характерное для индустриального общества, остаётся и в обществе информационном – в старых формах (например, на судоразборочных заводах Индии) и в новых (например, в гигантских кол-цен-

трах, где работники из развивающихся стран обслуживают потребителей из развитых).

Чтобы понять это сочетание преемственности и перемен, можно рассматривать XXI век через метафору «вирусного времени». Эта метафора помогает сосредоточиться на особенностях информационного общества, связанных с хактивизмом. Современные коммуникационные системы создают условия, в которых информация распространяется подобно вирусу, образуя «тёмные зоны» – места, где институциональный контроль становится всё труднее. Именно в этих «зонах» и возникает хактивизм.

Массовая культура, средства массовой информации и государственные структуры часто воспринимают эти явления с тревогой, преувеличивая угрозу и стигматизируя хакеров, что продолжает влиять на общественное восприятие хактивизма. Однако метафора вирусного времени также позволяет описать саму капиталистическую систему – её экспансию, адаптивность и уязвимость – и таким образом связать хакерство и хактивизм с более широким контекстом общества XXI века.

Восприятие технологической уязвимости существует в более широком общественном климате неуверенности, подпитываемом постоянным присутствием в новостях различных вирусных инфекций – от СПИДа и Эболы до трудноуловимых прионов в мясе, заражённом коровьим бешенством. Это создает культурно восприимчивую среду для тревог, со-

провождавших появление компьютерных супервирусов, что хорошо отражают газетные заголовки:

«Вirus Love Bug вызвал мировой хаос», The Guardian, 5 мая 2000 года;

«Новые вирусы “Love Bug” грозят новым бедствием», The Independent, 6 мая 2000 года;

«Супервирус угрожает ИТ-катастрофой», The Observer, 7 мая 2000 года;

«Остерегайтесь скрытных “сыновей Love Bug”», The Independent, 21 мая 2000 года.

Ранее хакеры, а теперь всё чаще и хактивисты, становились удобными козлами отпущения для этого чувства уязвимости, а также объектом страхов перед «неизвестным» и «чужим», которые некогда процветали во времена холодной войны, а теперь переродились в терминах «информационной войны». Парадоксальным образом, несмотря на абстрактную природу киберпространства, восприятие так называемой «техноуязвимости» часто выражается через метафоры, связанные с телесностью.

Форма и содержание самых сенсационных публикаций – например, знаменитой статьи Time под названием «Вторжение похитителей данных» – наглядно демонстрируют преемственность между современными медийными страхами и давними фобиями перед «вторжением в тело» – личное или национальное. Эти страхи характерны для параноидально-го стиля американской политической культуры и риторики

Пентагона времён холодной войны. В этих дискурсах всё пронизано идеей угроз телесной и технологической «иммунной системе»; каждое событие трактуется как манёвр в микробиологической войне, где метафоры черпаются и из генетики, и из кибернетики.

Подобные чувства уязвимости охватывают весь политический спектр, о чём свидетельствуют и левые критики «микрокибернетического потребительства». В одной из таких публикаций говорилось:

«Вызывает тревогу перспектива, что сопротивление микрокибернетической диктатуре потребления окажется возможным лишь в подполье – в руках фанатиков, готовых уничтожать, не вступая в диалог. А технологии этого типа особенно уязвимы для подобного рода оппозиции: как известно, хакеров ловят только тогда, когда они становятся слишком дерзкими, и вполне возможно, что уже сейчас где-то глубоко в системе действует группа компьютерных нигилистов, закладывающих свои вирусы, черви и бомбы».

Обычный уровень медийного ажиотажа, сопровождающий любое значимое событие, в случае хакерства и хактивизма усиливается тем, что эти явления связаны с трудно понятной для широкой публики областью вычислительной техники. Дополнительный эффект создают анонимность и нематериальный характер компьютерных действий. Всё это образует взрывоопасную смесь для тех, кто хочет сенсаций, а ранние хакерские сообщества лишь подливали масла в

огонь, выбирая вызывающие названия вроде Legion of Doom («Легион обречённых»), Bad Ass Mother Fuckers и Toxic Shock.

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.