СОДЕРЖАНИЕ

«Западные силы, настроенные против Китая, постоянно используют интернет, чтобы, как они говорят, свалить нас, и постоянно терпят поражение... То, насколько мы сможем отстоять свои интересы и победить в этой битве за интернет, напрямую скажется на идеологической и политической безопасности нашей страны».

Си Цзиньпин, из выступления
на Рабочей конференции по национальной
идеологии и пропагандистской работе,
август 2013 г.

Карта Китая, спорных территорий и специальных административных округов (Китайская Народная Республика, Гонконг, Тайвань, Макао)

Введение
ПЕРВЫЕ СИМПТОМЫ

Однажды в среду, в марте 2015 года в офисе IT-компании GitHub в Сан-Франциско прозвучала тревога. Древесный массив, много свободного места и естественного света — в общем, в помещениях компании господствовал тот самый бездушный скандинавский стиль, моду на который ввели в Кремниевой долине. Под сводом из мощных деревянных балок и алюминиевых воздуховодов барабанили по клавишам инженеры. Кто-то уже вышел из здания, но большинство еще собирались по домам. На улице стояла теплая ясная погода. Солнце только начинало садиться.

Сигнал тревоги не был для сотрудников GitHub чем-то из ряда вон выходящим. Для компании с 14 миллионами пользователей, на серверах которой хранился крупнейший в мире репозиторий компьютерного кода, жизненно важно, чтобы сервис был доступен круглосуточно и ни на секунду не выходил из строя. Разработчики в крупных и мелких компаниях по всему миру пользуются кодом на GitHub, каждую минуту тысячи пользователей загружают проекты, отмечают уязвимости и баги, выпускают новые версии программ и приложений. Короче говоря, если GitHub упадет, об этом будут знать все.

Первое тревожное сообщение было о том, что по нескольким проектам на GitHub зафиксированы большие объемы входящего трафика. Причина могла быть в чем угодно: от выпуска крупного обновления до

чего-то гораздо более серьезного. При увеличении объемов трафика, угрожающего функционированию сервиса, выдавались бы новые тревожные сообщения.

В тот день так и случилось. Серверы GitHub обрушились из-за DDoS-атаки[1].

Чаще всего сайты «ложатся» из-за внезапного притока трафика. Не в силах обработать множество одновременно входящих запросов, серверы выходят из строя или переключаются на черепашью скорость. Например, в 2015 году сайт Эйфелевой башни упал из-за того, что в дудл Google в честь 126-й годовщины постройки башни была вставлена соответствующая ссылка, по которой одновременно перешли миллионы посетителей[2]. По такому же принципу устроена DDoS-атака, но при этом она всегда кем-то инициирована. В последнее время количество таких атак увеличивается по экспоненте с ростом числа ботнетов, или армии компьютеров-зомби, инфицированных вирусным кодом, с помощью которого хакеры осуществляют над ними удаленный контроль.

«GitHub стал жертвой крупнейшей DDoS-атаки в своей истории», — так почти через сутки после начала атаки написал в своем блоге главный разработчик компании Джесси Ньюленд[3]. Если судить по имеющимся в открытом доступе сообщениям о статусе серверов, в течение следующих пяти дней сервер GitHub падал девять раз[4]. Инженеры сервиса 120 часов пытались отразить атаку, а она, как гидра, приспосабливалась и становилась вдвое сильнее, как только казалось, что с ней удалось справиться. В компании GitHub отказались от официальных комментариев, но один сотрудник на условиях анонимности сказал мне: «с таким мы еще никогда не сталкивались».

Во внутреннем чате GitHub сотрудники делились опасениями, что с атакой придется разбираться еще

какое-то время. Была одна проблема: все использованные ими ранее методы подбирались под атаки, с которыми GitHub и другие компании уже имели дело. А эта атака была другой. Счет шел уже не на часы, а на сутки. Между инженерами GitHub и неизвестными организаторами атаки развернулось что-то вроде соревнования. Напряженная сверхурочная работа не оставляла команде GitHub времени подумать, кто скрывается за маской хакеров. Комментируя слухи, плодившиеся в интернете, представители GitHub повторяли: «Мы считаем, что цель атаки — заставить нас убрать с сайта определенный контент».

Николас Уивер, житель Беркли, университетского городка в двадцати минутах езды от Сан-Франциско, был уверен, что знает, кто стоит за атакой, — Китай. Уивер, лысеющий мужчина в очках, всегда ходит в рубашке поло, говорит четко и по делу. Когда-то он был астрофизиком, но потом заинтересовался компьютерной безопасностью. Сперва атака на GitHub не привлекла его внимания. Сайты компаний подвергаются DDoS-атакам чуть ли не каждый день, да и GitHub уже сталкивалась с ними не раз. Но в интернете начали обсуждать, кто может быть неизвестным злоумышленником, и Уивер заинтересовался. Общаясь с другими экспертами по кибербезопасности в Twittere и блогах[5], он сузил радиус атаки до двух конкретных проектов на GitHub. Оба были связаны с GreatFire.org. Это китайская организация по противостоянию национальной интернет-цензуре. Выложенные на GitHub разработки предоставляли пользователям на территории Китая доступ к двум сайтам из черного списка — собственно сайту GreatFire и китайской версии сайта New York Times. GreatFire также входит в список иностранных антикитайских организаций по версии Управления по вопросам киберпространства КНР[6]. Сайт организации

уже давно подвергалась массированным DDoS-атакам и взломам. Поэтому ей пришлось перенести часть сервисов на GitHub, где они, по идее, должны были оказаться вне досягаемости.

Анализируя атаку, Уивер обнаружил доселе неизвестные элементы, которые могли иметь масштабные последствия для кибербезопасности. Совместно с Биллом Марчаком и еще семью исследователями в издательстве лаборатории Citizen Lab при Университете Торонто Уивер опубликовал работу, в которой утверждалось, что Китай разработал беспрецедентное кибероружие под названием «Большая пушка» (Great Cannon). Исследователи Citizen Lab проследили «Большую пушку» до инфраструктуры, которую использует Великий файрвол. Это гигантский аппарат интернет-цензуры, который отделяет интернет Китая от остального мира и контролирует, какие данные могут получать и передавать пользователи внутри страны.

«Факт успешного применения „Большой пушки“ представляет собой значительное достижение в области управления информацией на государственном уровне, — говорится в работе. — Цензура осуществляется путем передачи инструмента атаки в руки пользователей и нормализации широкомасштабных атак». Для атаки на GitHub «Пушка» использовала сервисы Baidu, одного из китайских интернет-гигантов. «Пушка» нашла уязвимость в системе онлайн-рекламы Baidu с миллионами показов по всему миру, перехватила трафик и перенаправила его на серверы GitHub. На тот момент сайт Baidu, которая, кстати, всячески отрицала свое участие в атаке, занимал четвертое место в мире по посещаемости. При каждом переходе на сайт с баннерами из системы Baidu код запрашивал данные с китайских серверов компании. Пока запрос обрабатывался, «Пушка» перехватывала фрагменты данных и заменяла

код Baidu на свой. При этом браузер пользователя начинал снова и снова обращаться к двум проектам на GitHub.

Атака перешла в долгую фазу. По данным команды Citizen Lab, ее последствия наблюдались вплоть до 8 апреля, или еще две недели после первого срабатывания тревожной системы GitHub. По подсчетам GreatFire, сайт которой тоже вышел из строя, за каждый день атаки им пришлось заплатить хостинговой компании более 30 000 долларов[7].

Пока разработчики GitHub пытались разобраться в атаке и ее последствиях и выработать план действий на будущее, специалисты по кибербезопасности ломали головы. Почему атака была такой масштабной? Зачем Китай действовал так нагло и топорно? «Это была демонстрация силы, — сказал мне Уивер. — Атака запускалась снова и снова, пока не сошла на нет». Принцип работы системы, описанный в документе Citizen Lab, был крайне изощренным, сопоставимым по сложности разве что с самим Великим файрволом. Организаторы взяли это сложное решение и начали долбить им по сайтам GreatFire и GitHub как отбойным молотком. Они явно хотели этим что-то сказать.

*

Где-то в то же время на другом конце мира другие люди тоже хотели что-то сказать.

В крохотной квартирке, едва втискиваясь в узкое пространство между шкафами и кухонным столом, толпились полицейские в голубых рубашках с расстегнутыми воротниками. Козырьки черно-белых фуражек надвинуты почти на глаза. От некоторых разило табаком, а пóтом разило от всех — кондиционер в квартире не справлялся с духотой из-за наплыва гостей.

Один из полицейских протянул Ли Гану[8] судебное постановление. Ли с ужасом ждал его вот уже несколько месяцев — с того самого момента, как начал украдкой на работе писать код для программы-антишпиона. С помощью этой программы любой пользователь мог перенаправить свой трафик через зашифрованный туннель, чтобы его нельзя было отследить или перехватить для анализа. Сравнить это можно с протоколом BitTorrent: его можно использовать легально, но большинство все равно незаконно скачивают по нему фильмы и сериалы. Так и программа Ли. Изначально ее задачей была приватность, но пользователи в Китае нашли ей другое применение. У них появилось решение, которое позволяло шифровать и маскировать трафик и наконец-то обойти Великий китайский файрвол.

«Не выполните постановление — пойдете в тюрьму», — сказал полицейский, вручая документ. Ли должен был немедленно прекратить работу над программой, а еще удалить все ее следы из интернета. «Х-хорошо», — пробормотал он. Внутри у него все похолодело. Три года работы псу под хвост. «У меня нет выбора. Я обязан подчиниться требованиям закона», — написал он в своем блоге, удаляя код программы.

В течение месяца китайская полиция пришла не только к Ли. Создателю GoAgent, другого инструмента обхода цензуры, Фус Лу тоже пришлось удалить свое детище. Он стер все свои твиты, кроме одного, со ссылкой на китайский перевод эссе Александра Солженицына «Жить не по лжи!». Эссе было написано 12 февраля 1974 г.[9]

> «Итак, через робость нашу пусть каждый выберет: остается ли он сознательным слугою лжи (о, разумеется, не по склонности, но для прокормления семьи,

для воспитания детей в духе лжи!) или пришла ему пора отряхнуться и стать честным человеком, достойным уважения и детей своих и современников»[10].

«Всему когда-то приходит конец», — написал Лу на сайте GoAgent. Он работал над программой четыре года.

GitHub, Фус Лу и Ли Ган стали одними из первых жертв на новом фронте войны Китая с интернетом. Ее развязало новое поколение цензоров, преследующих врагов государства любыми средствами, где бы они ни находились. Для многих сторонних наблюдателей история с GitHub стала первым признаком того, что за усилением цензуры стоит развитая идеология, которой КНР руководствовалась по отношению к национальному и международному сегментам интернета. Такой идеологией стала доктрина киберсуверенитета.

*

Никто не думал, что всё закончится так. Евангелисты интернета проповедовали абсолютную свободу от контроля государства. Всемирная сеть, говорили они, неподвластна цензуре, она обойдет и ее, а для репрессивных режимов станет настоящим ящиком Пандоры. Покойный киберлибертарианец Джон Перри Барлоу писал:

«Правительства индустриального мира, вы — утомленные гиганты из плоти и стали; моя же родина — Киберпространство, новый дом Сознания. От имени будущего я прошу вас, у которых все в прошлом: Оставьте нас в покое. Вы лишние среди нас. Вы не обладаете верховной властью там, где мы собрались».

Мы не избирали правительство, и вряд ли когда-либо оно у нас будет, поэтому я обращаюсь к вам, имея

> власть не большую, нежели та, с которой говорит сама свобода. Я заявляю, что глобальное общественное пространство, которое мы строим, по природе своей независимо от тираний, которые вы стремитесь нам навязать. Вы не имеете ни морального права властвовать над нами, ни методов принуждения, которые действительно могли бы нас устрашить»[*].

Утопическая риторика Барлоу и его соратников прошла даром. Неосвоенные пространства молодого интернета запестрели огороженными участками. Их застолбила горстка пионеров индустрии, заработав миллиарды на новой сетевой монополии. Продвигая принцип «Информация хочет быть свободной», компании Кремниевой долины изо всех сил сопротивлялись централизованному регулированию и антимонопольному законодательству. Хотя интернет сам по себе создавался под патронатом и финансированием государства, этот факт старательно скрывали. Так в Сети восторжествовала частная инициатива, а любые законодательные ограничения были для нее смертельной угрозой.

Сегодня мы наблюдаем закат этой идеологии. Средствами массовой информации и политикой управляют IT-корпорации. Независимые СМИ, если они еще остались (что свело бы на нет ключевую функцию средств массовой информации — надзор за крупным капиталом), можно утихомирить, слегка изменив какой-нибудь важный алгоритм. Несметные богатства Кремниевой долины развратили современную политику: избранники народа вынуждены ползать на коленях перед хайтек-миллиардерами, изыскивая для людей рабочие места, которые отобрали дата-центры, штаб-

[*] Перевод с английского Евгения Горного. Опубликовано в Zhurnal.ru #1, 02.10.1996. — *Прим. науч. ред.*

квартиры корпораций и гиг-экономика*. Операторы социальных сетей отказываются исполнять обязанности издателей и охранников, и на плодородной почве социальных сетей пышным цветом цветут дезинформация и пропаганда, отравляя все вокруг себя ложью и ненавистью. Они превращают миллионы людей в радикалов и даже могут влиять на результаты выборов.

Момент истины близок. Все чаще раздаются призывы поставить интернет под контроль, обуздать неограниченную власть IT-индустрии. Но здесь та же ситуация, что и с капитализмом и демократией. Капитализм настолько плотно завязан на концепции демократии, что проблемы с первым иногда считают поводом отказаться от последней. Точно так же крах киберлибертарианского статус-кво Кремниевой долины грозит утратой ценностей открытого и свободного интернета.

Существует альтернативная концепция интернета, Она гораздо более последовательна и убедительна, чем многим из нас хотелось бы. Китайская доктрина кибersуверенитета не считает интернет уникальной технологией, выходящей за рамки государственных границ и международного контроля. Согласно этой доктрине, интернет ничем не отличается от других технологий и поэтому подлежит регулированию. В физическом мире действуют правила пограничного контроля и таможенные пошлины. Почему тогда цифровая сфера должна быть на особых правах? Доктрина киберсуверенитета — это концепция тотального контроля над интернетом, продиктованная крайним недоверием ко Всемирной сети и подозрением, что она представляет собой опасность для государственной власти.

---

* Гиг-экономика — бизнес-модель компаний типа AirBNB, Uber и пр., построенная на использовании временного труда или временного предоставления личных ресурсов. — *Прим. науч. ред.*

Западному сознанию китайская цензура вот уже много лет представляется чем-то вроде страуса из аналоговой эпохи, прячущего голову в цифровой песок. Однако ее видение будущего оказалось ближе к реальности, чем у их противников, защитников свободы интернета. Цензоры интернета в Китае справедливо указывают на разгул фейковых новостей, ненависти в социальных сетях, атаки хакеров и утверждают, что для Китая такие проблемы неактуальны. Это отчасти правда. Великий китайский файрвол — колоссальная машина цензуры, которая контролирует китайский интернет во всех его проявлениях, предлагает пользователям чувство безопасности, защищенности от неотфильтрованного сетевого хаоса, кишащего террористами, педофилами, хакерами и мошенниками.

Коммунистическая партия Китая неоднократно успешно доказывала, что способна справиться с любым кризисом, будь то катастрофические последствия ее же собственной политики — от Большого скачка до культурной революции, или же «арабская весна» и финансовый кризис 2008 года. Китайские цензоры из раза в раз доказывают, что умеют адаптироваться к тактике противников и перехитрить их. Они создали самую совершенную в мире систему фильтрации, контроля и наблюдения за интернетом. И эта система только набирает обороты. Китайских и иностранных технологических гигантов заставили ходить по струнке, а тех, кто отказался сотрудничать, изгнали. Пропаганда проникла во все сферы жизни, агрессивная шовинистическая риторика задавила собой любую критику государственного контроля.

Невзирая на указанные достижения, техноутописты продолжают считать панацеей от цензуры последние интернет-технологии: блоги, социальные сети, мессенджеры. Любая уязвимость или брешь в Великом