



Сергей
ГОЛУБИЦКИЙ
специально
для «Новой»

На портале журнала Wired — культового прожект интеллектуалов, влюбленных в информационные технологии, есть закрепленный раздел Most Popular. В первой пятёрке самых популярных публикаций, в окружении сплошь свежих статей, устойчиво висит текст Энди Гринберга, озаглавленный «Как целая нация превратилась в тестовую лабораторию России по ведению кибервойны», написанный в июле 2017-го.

Стало любопытно: это что же нужно такое написать, чтобы тема не отпускала многомиллионную аудиторию Wired почти полтора года?!

В статье Гринберга рассказывается о том, как ровно в полночь накануне Нового, 2016-го года в Киеве погас свет. Главный герой — специалист по украинской кибербезопасности, вспомнил, что в декабре 2015 года (опять-таки в полночь) свет тоже погас. Было очень холодно и из-за нарушения в подаче электроэнергии трубы отопительной системы едва не лопнули, а люди едва не замерзли.

Несмотря на то что свет зажали уже через пару часов, специалист по украинской кибербезопасности сразу догадался: работают русские хакеры. Почему? Свет, может быть, и гас лишь дважды за два года, зато все остальное время страну непрерывно преследовали цифровые апокалиптические омены: в СМИ и на электростанциях, в транспортных и военных структурах, у политиков и аналитиков постоянно ломались компьютеры, исчезали файлы, самопроизвольно стирались данные.

Президент Порошенко прямо сказал: «За два последних месяца на 36 украинских объектах было произведено 6500 кибератак». Международные специалисты по кибербезопасности из-за отсутствия достаточных доказательств ограничились намеками, но у президента Порошенко сомнений не было: «Расследования украинских экспертов однозначно указывают на прямую или косвенную вовлеченность российских спецслужб, развязавших кибервойну против Украины».

Далее Гринберг обстоятельно излагает подробности взломов украинских компьютеров, описывает запертые загрузочные сектора жестких дисков и сокрушается о неспособности антивирусных программ противостоять саранче из Пятой печати грядущего киберапокалипсиса, явившейся в образе червя KillDisk и трояна BlackEnergy.

В 2014 году калифорнийская компания FireEye, специализирующаяся на кибербезопасности, возложила вину за распространение вредоносного кода KillDisk и BlackEnergy на территориях Польши и Украины на российскую хакерскую группу Sandworm, и эта версия впоследствии легла в основу официальной американской позиции.

С тех пор американские специалисты рука об руку с украинскими коллегами денно и нощно изучают подрывную деятельность «кремлевских хакеров» на Украине, которую, как объясняет Гринберг, Россия превратила в тестовый полигон для будущей кибервойны против Соединенных Штатов и остальных стран свободного мира.

Такая вот вышла статья у Энди Гринберга, наполненная сочным макабром и оттого пользующаяся заслуженной популярностью у технической интеллигенции.

Зачем, спрашивается, я вспомнил в ноябре 2018-го кибератаки на Украину двухлетней давности, хорошо изученные и подробно описанные? Затем, что статья Гринберга грубо деформирует истину, причем сразу по двум направлениям — информационному и временному.

Смысл информационной деформации заключается в проталкиваемой читателям Wired иллюзии, согласно которой цифровой апокалипсис ведет лишь один — русский — всадник.

Смысл временной деформации — в представлении о кибервойне как о чем-то грядущем, ожидаемом в будущем.

Из уважения к интеллектуальному потенциалу читателей «Новой» мне бы хотелось расставить правильные акценты в этой теме и уберечь нас всех от пропагандистской примитивизации, которую навязывает статья Гринберга.

Начну с временной деформации. Реальность такова, что кибервойна не вот-вот начнется, а ведется уже давным-давно, едва ли не с рождения Мировой паутины.

Романтики вроде Тима Беренса-Ли задумывали Web как *позитивное цифровое пространство*, в котором люди смогут реализовывать свой творческий потенциал и обмениваться возвышенными импульсами. Предполагалось, что виртуальное сообщество станет альтернативой пако-стям реальной жизни.

Случилось, однако, то, что только и могло случиться: интернет стал банальным отражением реальной жизни, а злая природа человека проявилась в нем с удвоенной силой благодаря анонимности и безнаказанности.

В 90-е годы цифровое сообщество училось сбиваться в волчьи стаи и оттачивало специфические орудия ведения враждебных действий в духе Томаса Гоббса (*bellum omnium contra omnes*). В нулевые анархия закончилась и произошло структурирование цифрового пространства на принципах национального и геополитического *суверенитета*.

Еще в 30-е годы прошлого века немецкий философ Карл Шмитт дал замечательное определение *суверена* как «того, кто принимает решение о чрез-

«Американцы выпустили джинна из бутылки, поэтому подключение к гражданской войне за суверенные права России и Китая было лишь вопросом времени»

вычайном положении». Для того чтобы национальные и транснациональные элиты могли реализовывать собственные претензии на власть, требуется «чрезвычайное положение», которое в идеале устраивать не в родном государстве, а на обособленной территории — «двойственной и неясной зоне, на пересечении юридического и политического».

Создание подобной *внеправовой территории* позволяет сохранять видимость приличия и творить при этом чудовищные беззакония. Итальянский философ Джорджио Агамбен удивительным образом предсказал *неизбежность появления*

Если завтра



Секьюрети-Мен и Клауд-Вумен — персонажи конференции по кибербезопасности, США

в современном обществе островов «правового беспредела» за 6 лет до 11 сентября 2001 года.

Специфика тюрем вроде Абу-Грейб и Гуантанамо как территорий «чрезвычайного положения» в том, что в них можно пытаться и содержать без суда и следствия, оставаясь при этом в рамках демократического общества и правового государства. Именно по причине *экстерриториальности* этих тюрем и *чрезвычайности* ситуации.

Уже упомянутый Джорджио Агамбен в монографии *Homo Sacer* иллюстрирует важность «чрезвычайного положения» для реализации *суверенных амбиций* «Декретом о защите народа и государства», который Адольф Гитлер издал сразу после прихода к власти (28 февраля 1933 года).

Этот декрет позволил нацистской власти формально не отменять Веймарскую республику, и при этом вносить поправки в Конституцию в плане урезания личных свобод. Завабно, что «декрет никогда не был отменен, что с юридической точки зрения позволяет считать Третий рейх чрезвычайным положением, длившимся 12 лет».

История нам показала, что у беззаконий, творимых под прикрытием «чрезвычайного положения», нет пределов.

После глобального переворота в мировом порядке, случившегося 11 сентября 2001 года, *интернет стал экстерриториальной площадкой*, идеально подходящей для любого «беспредела» под прикрытием риторики о «чрезвычайном положении».

Читатель уже догадался, что эта риторика родилась из жупела «между-

народного терроризма» и фантома бен Ладена. Американцы выпустили джинна из бутылки, поэтому подключение к гражданской войне за суверенные права игроков, ранее находившихся на обочине истории, — России и Китая, было лишь вопросом времени.

Полноценная и широкомасштабная кибервойна началась не в декабре 2015 года на Украине, а в 2001 году после принятия «Закона о патриотизме» — неслыханной в истории американской демократии инициативы, поправшей большую часть свобод, которые отвоёвывались американским гражданским обществом на протяжении столетий. И все это под прикрытием «чрезвычайного положения» и «защиты национальных интересов».

Несколько лет российские и китайские властные элиты с восхищением наблюдали за работой старшего брата, кульминацией которой стал киберчервь Stuxnet, разрушивший 1000 (!) ядерных центрифуг на заводе по обогащению урана в иранском Нетензе (совместная израильско-американская операция «Олимпийские игры»).

Апокалиптическая картина понравилась — и понеслось. Примитивные DoS-атаки из арсенала нулевых (2007-й в Эстонии, 2008-й в Грузии, 2009-й в Киргизии) сменились высокопрофессиональной точечной деструкцией последней пятилетки: взлом серверов немецкого парламента в 2015-м, в результате которого мир узнал (и быстро забыл) о фактах слежки американского Агентства национальной безопасности за немецкими политиками высшего эшелона; вредоносное ПО

