Текст · 13 декабря 2022, 14:12
Economist,

Как Россия проигрывает кибервойну в Украине. Разбирается журнал Economist

Россия ведет кибервойну против Украины уже много лет — и атаки усилились с первых часов полномасштабного вторжения в феврале. Но ожесточенность кампании несоизмерима с ее эффективностью. Журналисты *Economist* проанализировали, какие уроки можно извлечь из неудач России на киберфронте. «Медиазона» публикует перевод этой статьи.

Подготовка поля битвы

В 331 году до н. э. в битве при Гавгамелах персидский царь Дарий приказал рассыпать по полю шипы — там, где он предполагал основное наступление кавалерии Александра Македонского. В 1944-м союзники готовили свое поле битвы немного иначе: с помощью муляжей десантных судов и самолетов они хотели убедить немецкое командование, что их наступление будет в Па-де-Кале, а не в Нормандии. 24 февраля Россия попыталась сделать что-то подобное: меньше чем за час до того, как российские танки въехали на территорию Украины и устремились к Киеву, хакеры взломали спутниковую связь *Viasat*, на которую полагались украинские военные.

Виктор Жора, заместитель председателя Государственной службы специальной связи и защиты информации Украины, еще в марте

признавал, что в результате «имели место серьезнейшие перебои с коммуникацией в самом начале войны». Бывший руководитель одной из подобных западных служб считает, что такая атака требует «года или двух очень тщательной подготовки».

Кто-то выигрывает, кто-то нет. Союзники победили. Высадка в Нормандии была успешной. Дарий проиграл и потерял свое царство. Так и российская атака на Киев была отбита. Несмотря на все затраченные усилия, Россия не смогла напустить достаточно плотного тумана войны с помощью хакеров. И это любопытно. Кибервойна была упорной. И Украина должна была стать испытательным полигоном для этой новой формы боевых действий. Но средства ведения этой новой войны, судя по всему, пока не достигли тех высот, которых от них ждали.

Битва за биты

Российская атака на *Viasat* была не единственной попыткой ослабить противника через программное обеспечение. Еще в январе, а потом и 23 февраля в сотнях украинских систем были обнаружены вредоносные программы, так называемые вайперы, которые уничтожают данные. В апреле, когда угрожавшие Киеву войска отступили, хакеры из группы *Sandworm*, которую западные эксперты и спецслужбы связывают с российским ГРУ, использовали вредоносную программу *Industroyer2* для атаки на электростанции.

Такого рода атаки на гражданскую инфраструктуру сложно не заметить. Но с военным оборудованием дело обстоит иначе. ВСУ сохраняют высокий уровень секретности и не сообщают, какие из их линий связи были нарушены или взломаны (а это точно происходило). Но видимый эффект российской киберкампании в любом случае удивительно невелик. «Честно говоря, мы думали, что воздействие будет значительно более масштабным, — сказала 16 ноября высокопоставленная сотрудница Пентагона Мике Оянг. — Российские кибервойска, как и традиционные вооруженные силы, не превзошли ожидания».

В первые дни войны Украина оставалась в сети. Электричество работало, даже когда вокруг столицы шли ожесточенные бои. Были открыты банки. В отличие от 2015 и 2016 годов, когда кибератаки приводили к массовым отключениям электричества, ток продолжал бежать по проводам. И информация тоже. Ничто по-настоящему не мешало Владимиру Зеленскому каждый вечер обращаться к украинскому народу. Если Россия пыталась подорвать доверие украинцев к своему правительству и сделать страну неуправляемой, у нее это не вышло.

И тут главную роль сыграла украинская оборона. Директор Национального центра кибербезопасности Британии *(NCSC)* Линди Кэмерон считает, что натиск российских хакеров был, «возможно, самой упорной и напряженной из зафиксированных кибератак». Но, как писал сэр Джереми Флеминг, ее начальник и руководитель британского Центра правительственной связи *(GCHQ)* в

своей августовской статье для *Economist*, ответ Украины был, «пожалуй, самым эффективным в истории сопротивления кибератакам». Россия годами отрабатывала на Украине кибероперации. Так, *Industroyer*, предшественник *Industroyer2*, вызвал блэкауты в 2016-м. И это дало украинским властям представление о целях российских атак и время на укрепление инфраструктуры.

Это значит, что к началу вторжения у украинского киберкомандования был продуманный план действий. Некоторые чиновники выехали из Киева в более безопасные части страны. Другие заняли командные пункты на линии фронта. Ключевые службы были выведены в дата-центры в Европе, вне радиуса российских ракет. Украинские вооруженные силы знали, что спутниковая связь может прерваться, и подготовили другие виды связи. В итоге атака на *Viasat* «не имела никакого принципиального воздействия на связь внутри ВСУ», утверждал Виктор Жора в сентябре — и тем самым дезавуировал собственные более ранние высказывания.

Помощь друзей

Огромную роль сыграла и помощь Запада.

Одним из способов, которым НАТО увеличивало взаимодействие с Украиной перед войной, был доступ к библиотеке киберугроз, хранилищу известных на тот момент вирусов. Британия предоставила поддержку на 6 млн фунтов, включая файрволы, чтобы блокировать атаки, и экспертов для анализа вторжений. Помощь была взаимной. «Вероятно, от украинцев США и Британия узнали о российских

хакерских тактиках больше, чем украинцы узнали от них», — отмечает Маркус Уиллет, который раньше отвечал в *GCHQ* за вопросы кибербезопасности.

Парадоксальным образом украинскому сопротивлению помогло то, что многие промышленные системы управления были унаследованы от СССР и оказались технически отсталыми. Когда, например, *Industroyer* ударил по электрическим подстанциям Киева в 2016 году, инженеры смогли перезапустить систему вручную всего за несколько часов. Когда *Industroyer2* в апреле отключил часть электросети, она вернулась к работе через четыре часа.

Поучаствовали в помощи Украине и частные компании, занимающиеся кибербезопасностью. Жора говорит, что особенно важную роль сыграли *Microsoft* и словацкая фирма *ESET*, которые широко представлены в сетях Украины и, соответственно, способны собирать телеметрию, или сетевые данные. Сведения, предоставленные *ESET*, позволили кибероборонe Украины отбить атаку *Industroyer2*. *Microsoft* утверждает, что искусственный интеллект, который может сканировать программу быстрее человека, также позволил оперативно отслеживать нападения. 3 ноября президент *Microsoft* Брэд Смит объявил, что его фирма будет до конца 2023 года бесплатно осуществлять техподдержку Украины. Таким образом, размер помощи компании Украине с февраля 2022 года составит больше $400 млн.

Украина оказалась крепким орешком. Но не была ли при этом преувеличена мощь российских

хакеров? У разведки в России огромный опыт кибершпионажа, но военные киберсилы довольно «молоды» по сравнению с западными противниками, говорит Гэвин Уайлд, который раньше курировал российское направление в Совете национальной безопасности США. Америка начала внедрять элементы кибервойны в свои операции еще в 1990-е, во время конфликтов на Гаити и в Косово. Россия занимается этим только в последние шесть лет, утверждает Уайлд.

Американские, европейские и украинские официальные лица говорят, что есть много примеров, когда российские кибератаки синхронизируются с атаками физическими. Но есть и примеры грубейших ошибок. Сэр Джереми Флеминг говорит, что в некоторых случаях российские военные бьют по той же сети коммуникаций, которую пытались взломать кибервойска, и это заставляет украинцев обращаться к более защищенным способам коммуникации.

Есть и те, кто считает, что российские киберсилы довольно расхлябанно себя ведут: хорошо умеют ломать, но делают это неточно и привлекая к себе излишнее внимание. В апреле Дэвид Каттлер, помощник генсека НАТО по вопросам разведки и безопасности, отметил, что Россия использовала против Украины больше разрушительных вредоносных программ, «чем запускают за год все мировые киберсилы вместе взятые».

Но судить об успехе киберкампании по количеству вирусов — это все равно что оценивать пехоту по

числу стреляных гильз. Дэниел Мур, автор недавно вышедшей книги «Наступательные кибероперации», пишет, что все до единой атаки России на инфраструктуру в Украине не только были вычислены заранее, но и проведены с огромным количеством ошибок или затронули совсем не те объекты, которые планировалось. Ровно так было в случае с *NotPetya* — самораспространяющейся программой-вымогателем, запущенной в 2017 году, которая вышла за пределы Украины и нанесла ущерб в $10 млрд по всему миру.

«Почти в каждой атаке, которую Россия осуществляла в киберпространстве, были существенные операционные провалы», — говорит Мур. В качестве обратного примера он приводит *Stuxnet*, израильско-американскую кибератаку на иранский ядерный объект, впервые обнаруженную 12 лет назад — с точки зрения технологий «прошлый век»: «И тем не менее она была устроена гораздо сложнее, чем все, что мы видим сегодня со стороны России».

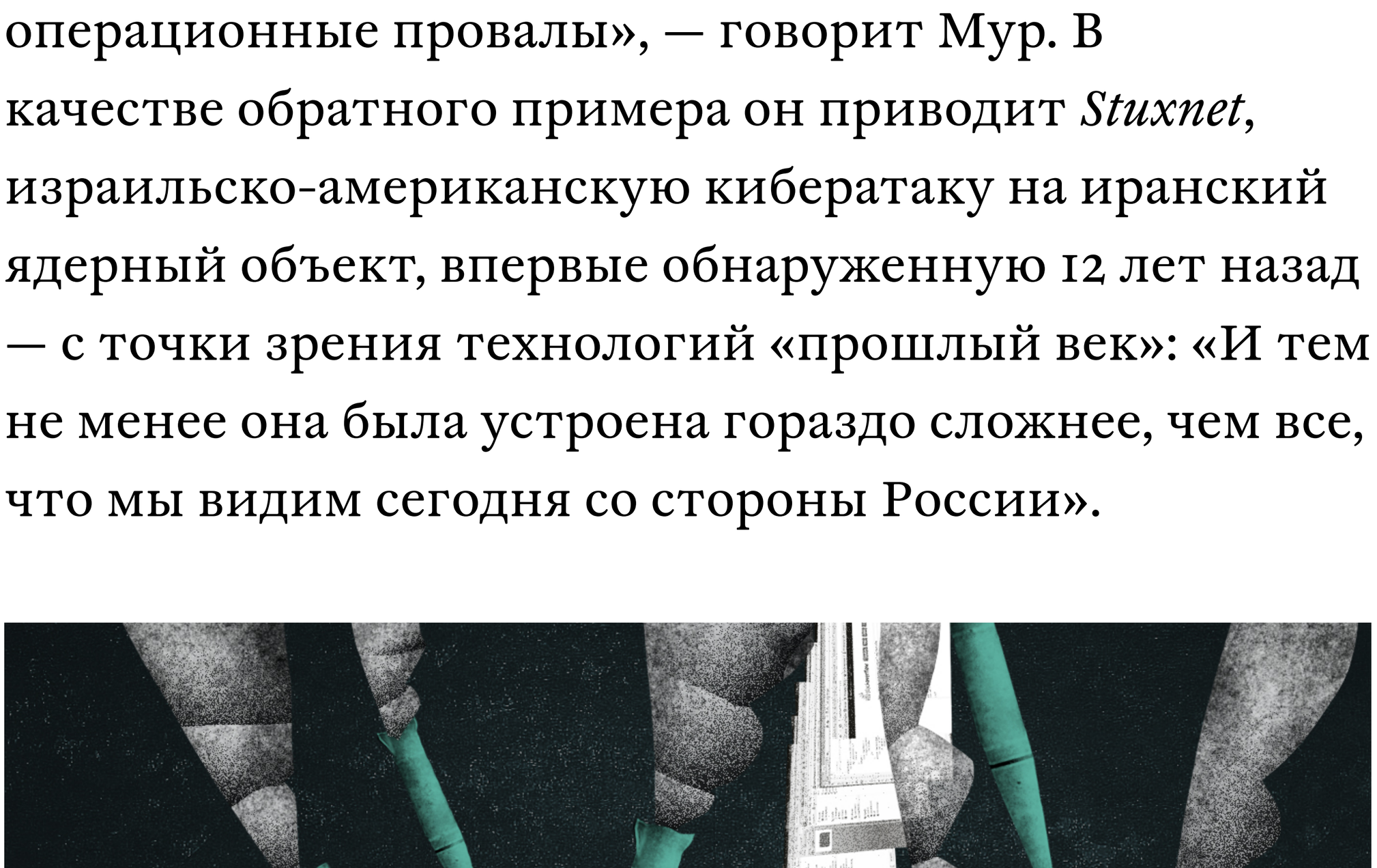

Иллюстрация: Ника Кузнецова / Медиазона

Реальное и виртуальное

Многие представители западного разведывательного сообщества говорят, что война показывает пропасть между кибервойсками России и той же Америки. Эффективность их атак против военной техники несопоставима. Но другие предупреждают, что делать далеко идущие выводы слишком рано. Российская киберкампания, возможно, проходит неудачно не из-за низкого уровня подготовки, а из-за высокомерия, которое свойственно и обычной армии России.

Западные чиновники говорят, что Россия не смогла спланировать и запустить по-настоящему разрушительные кибератаки на энергетическую и транспортную системы Украины не потому, что не была на это способна в принципе, а потому, что предполагала, что скоро захватит страну — и вся эта инфраструктура будет принадлежать ей. Зачем уничтожать то, что тебе самому скоро понадобится? Когда стало очевидно, что война будет затяжной, России пришлось адаптироваться. Но кибероружие не похоже на обычное, которое ты можешь просто перенаправить на другую цель и снова открыть огонь. Его нужно специально подгонять под конкретные цели.

Сложные атаки, такие как нападение на *Viasat*-, требуют серьезнейшей подготовки, в том числе подробнейшего изучения работы сетей. Леннарт Машмайер, старший научный сотрудник Центра исследований безопасности *ETH Zurich*, в своей прошлогодней статье показал, что атака ГРУ на электросеть Украины в 2015 году потребовала 19

месяцев подготовки, а в 2016-м — 2,5 лет. Кроме того, после таких атак противник получает представление о средствах (то есть коде) и инфраструктуре (серверах) нападающей стороны, что нивелирует их эффективность в будущем.

После первой недели войны кибератаки России стали более тактическими и случайными. В апреле, когда российская армия переключилась с киевского направления на Донбасс, количество нападений вайпер-программ резко упало. В ноябре исследователи из *Mandiant* — компании, занимающейся кибербезопасностью, — сообщили, что теперь ГРУ сосредоточилось на выводе из строя периферийных устройств, таких как роутеры, файрволы, почтовые серверы. Это более быстрые атаки, но их гораздо сложнее скрыть.

«То, что вы видите, — это кривая границы производственных возможностей, — говорит Джон Вольфрам из *Mandiant*, ссылаясь на постулат экономической теории, описывающий различные комбинации двух товаров, которые могут быть произведены с использованием имеющихся ресурсов. — У вас есть определенное количество знаний и капитала, и вы должны решить, потратите вы их на одну-две высокоточные операции или на 50 более простых». Выбор последнего совершенно не значит, что первое вам недоступно. «Россия совершенно точно способна на кибератаки более высокого уровня, чем демонстрируют нам события в Украине», — отмечает Каттлер. «Война еще не дошла до стадии, когда обе стороны начинают обрушивать друг на

друга всю свою кибермощь», — соглашается с ним Маркус Уиллет.

Возможно, мы еще увидим эту кибермощь. Диверсия на «Северном потоке» и «Северном потоке — 2» в сентябре, а также ракетные удары по энергосети Украины говорят о том, что Кремль начинает вести все более рисковую игру. Это видно и в киберпространстве. Один британский чиновник считает, что Россия, помня об инциденте с *NotPetya*, сначала очень старалась, чтобы атаки затрагивали только Украину, — ссориться с НАТО ей вовсе не хотелось. Но, возможно, это уже не так. В прошлом сентябре хакерская группа *Sandworm* впервые намеренно атаковал страну НАТО. Речь о *Prestige*, вредоносной программе, целью которой являлась транспортно-логистическая система в Польше, которая сейчас стала центром распределения военной помощи Украине.

Есть и те, кто считает, что мощь кибервойны вообще неверно оценивается. «Кибероперации действительно были интенсивными и сыграли существенную роль», — признает Кьярен Мартин, предшественник Кэмерон в *NCSC*. Но война показала, что «в период активных боевых действий у кибератак есть серьезные ограничения». *Stuxnet*, который проник в иранские системы, физически не подключенные к интернету, нанес серьезный вред, но при этом его месяцами никто не замечал. Успех операции в Иране дал ложное представление о том, что кибератаки — это такое новое чудо-оружие, которое может заменить бомбы и ракеты. На самом деле, считает Мартин, *Stuxnet* был «высадкой на

Луну» в киберсфере, исключительным и уникальным событием, которое потребовало гигантских ресурсов для воплощения, а не рядовой атакой в кибервойне.

Не стоит считать кибератаки «волшебным невидимым полем боя, где ты безнаказанно можешь делать что угодно», говорит Мартин. Во-первых, очень сложно по-настоящему нарушить работу хорошо защищенных компьютерных систем. Во-вторых, эти атаки, вопреки сложившемуся мнению, «легко вычислить». Кибернападения не проходят без последствий. «Несмотря на весь хайп, — отмечает Мартин, — с начала вторжения Путин не особо напугал Запад в киберпространстве».

Чтобы разрешить этот спор и сделать выводы, потребуется время. К тому же многие атаки могли пройти незамеченными. Например, нападение на львовскую региональную военную организацию засекли очень поздно, и коммерческое программное обеспечение, по сути, так и не смогло вычислить, как именно сработал российский вирус. Вычисление атак — наука неточная, говорит украинский чиновник в сфере кибербезопасности. Зачастую в систему входят совершенно законно, просто по украденному паролю. Видны только симптомы, а не причина. «Это как если вы видите человека с кашлем и низким уровнем кислорода в крови, — говорит Мартин. — Сейчас-то мы уже понимаем, что это может быть ковид. С вредоносными программами похоже. Мы редко замечаем момент, когда они проникают в сеть, и узнаем их, только когда видим отклонения. В большинстве случаев мы ловим атаку где-то в середине процесса».

К тому же самые разрушительные кибероперации, такие как *Stuxnet*, гораздо актуальнее в мирное время. Во время военных действий традиционное оружие может произвести те же разрушения гораздо быстрее и дешевле. Наверное, самой важной киберактивностью в войну с обеих сторон можно назвать операции, направленные на сбор разведданных или психологическую войну.

Бывший высокопоставленный чиновник в правительстве Украины, у которого остается доступ к закрытой информации, подтверждает, что самый ценный вклад киберсил страны в войну — это выведывание секретов, например данных европейских компаний, которые обходят американские санкции против России. «Я не могу раскрывать подробности, но это потрясающая работа», — говорит он. О том, что союзники смогли расшифровать немецкие «Энигмы», шифровальные машины времен Второй мировой, стало известно только в 1970-х. Совокупный эффект киберопераций в Украине может еще на годы остаться под завесой тайны.

Оригинал: *Lessons from Russia's cyber-war in Ukraine*, *The Economist, November 30, 2022*

Перевод: Вера Нифлер