ОТЧЕТ ПО **КИБЕРБЕЗОПАСНОСТИ**

IT-армия Украины
Структура, постановка задач и экосистема

Штефан Соесанто

Цюрих, июнь 2022 года
Центр исследований безопасности (CSS), Швейцарская высшая техническая школа Цюриха (ETH Zürich)

CSS
ETH Zürich

ETH zürich

Доступно по ссылке:
css.ethz.ch/en/publications/risk-and-resilience-reports.html

Автор: Штефан Соесанто

Управление проектом со стороны ETH-CSS: Мириам Данн Кавелти, заместитель руководителя по исследованиям и обучению; Андрин Хаури, руководитель группы рисков и устойчивости; Андреас Венгер, директор CSS.

Редактор: Тейлор Гроссман
Макет и графика: Мириам Дахинден-Ганцони

DOI: 10.3929/ethz-b-000552293

Содержание

1 Введение

За несколько лет до начавшегося 24 февраля 2022 года российского вторжения в правительственных кругах Украины возникла общая идея создания добровольческой киберармии. Отчасти эти рассуждения были подкреплены информацией об успехах Киберподразделения Союза обороны Эстонии и аналогичных мер по всему миру, направленных на организацию и интеграцию гражданских IT-добровольцев в существующие военные структуры и их активизацию в нужное время.

В отличие от этих хорошо зарекомендовавших себя и сугубо оборонительных усилий по привлечению кибердобровольцев, IT-армия Украины была мобилизована стихийно, без четко структурированного и проверенного плана. Это, а также факт отсутствия у Украины военного киберкомандования, заставило Киев творчески решать задачу по объединению своих зарождающихся военно-разведывательных кибермощностей с огромным и полным энтузиазма глобальным гражданским IT-сообществом в целях обороны страны. Рожденная из необходимости, IT-армия впоследствии превратилась в гибридный конструкт, не являющийся по своей природе ни гражданским и ни военным, ни государственным и ни частным, ни локальным и ни международным, ни законным и ни незаконным.

На момент написания данной статьи IT-армия состоит из двух частей: (1) постоянный, глобальный призыв к действию, который мобилизует любого, кто готов участвовать в скоординированных DDoS-атаках против определенных – в первую очередь гражданских – объектов российской инфраструктуры; и (2) группа собственных специалистов, вероятно, состоящая из сотрудников украинского оборонного ведомства и разведки, которые проводят эксперименты со все более сложными кибероперациями против конкретных российских целей. Обе части IT-армии, по своей природе, являются чисто наступательными и служат для объединения добровольцев-любителей (гражданских лиц) и обученных профессионалов (гражданских, военных, разведчиков) в одну – скорее всего – иерархически организованную структуру.
Кроме того, IT-армия также способствовала формированию экосистемы, в которую входят принадлежащие Украине IT-компании и отдельные лица, расположенные за пределами Украины, а также украинцы, живущие на Украине и работающие на западные компании. Данная экосистема постоянно создает новые инструменты, генерирует ноу-хау, выявляет новые цели и выполняет другие функции разведывательного обеспечения, чтобы поддержать наступательные усилия Украины в киберпространстве.

Зачем нужно военное киберкомандование, если у вас есть IT-армия?

Структура и сила притяжения IT-армии ставят перед международным сообществом множество новых проблем в таких областях, как, например, применение международного права в киберпространстве, законодательные инициативы государств, атаки на гражданскую инфраструктуру, а также этическое поведение IT-компаний со штаб-квартирами за пределами Украины. Многие – если не все – из этих проблем в значительной степени игнорируются исследователями и сообществом специалистов по информационной безопасности, а также политиками как в государствах-членах ЕС, так и в НАТО. До конца неясно, почему это происходит именно так, но, похоже, политическая и идеологическая поддержка Украины, с одной стороны, и растущие антироссийские настроения, с другой, создали среду, в которой поведение украинцев в киберпространстве умышленно игнорируется, поверхностно анализируется, или значительно преуменьшается с точки зрения его воздействия и значимости.

Что касается DDoS-атак, то в части поведения IT-армии наблюдается множество стратегических совпадений с DDoS-кампанией против Эстонии в мае 2007 года. Кампания 2007 года была организована русскими националистическими хактивистами через русскоязычные форумы/веб-сайты и длилась 22 дня. По сей день не появилось никаких четких доказательств участия российского правительства, поэтому кампания никогда официально не приписывалась российскому государству. В результате критики со стороны Эстонии и западных стран, было привлечено внимание к вопросу о том, что Москва не предприняла никаких значимых мер для смягчения последствий этой DDoS-атаки (нарушение ею обязательства проявлять должную осмотрительность), а отсутствие сотрудничества при проведении расследования Эстонией стало одним из доказательств того, что российское правительство защищает – и тем самым косвенно поддерживает – лиц, ответственных за DDoS-кампанию. В этой обстановке всеобщей беспомощности спикер эстонского парламента Эне Эргма даже произнесла ставшую известной фразу: «Когда я думаю про ядерный взрыв и смотрю на взрыв, произошедший в нашей стране в мае, я вижу одно и то же».[1]

При этом, в отличие от 2007 года, действия IT-армии в части DDoS-атак довольно прозрачны, если говорить об их авторстве, правительственных полномочиях, инструкциях, руководстве и контроле. Столь же очевидно, что IT-армия настойчиво и целенаправленно атакует российскую гражданскую инфраструктуру, включая интернет-аптеки, банки, службы доставки продуктов питания и розничные сети. Но в то время, как Россию справедливо осуждают за DDoS-атаки 2007 года, IT-армия и министр цифровой трансформации Михаил Федоров получили две награды на Европейском форуме кибербезопасности CYBERSEC 2022 в Катовице, Польша, за «героическое сопротивление российской агрессии и защиту цифровых границ

[1] Кевин Поулсен, «“Кибервойна” и паническая атака Эстонии», *Wired*, 22 августа 2007 г., https://www.wired.com/2007/08/cyber-war-and-e/.

демократического мира».[2] Как выразился Федоров: «Эта награда в первую очередь для всего киберсообщества и добровольцев, которые сейчас ведут вместе с нами первую в истории кибервойну».[3] Хотя, безусловно, существует разница между DDoS-кампаниями, проводимыми в мирное время и во время войны, похоже, что Запад сейчас выбрасывает за борт правовые и юридические толкования, которые он отстаивал в киберпространстве в течение последнего десятилетия ради политической поддержки Украины.

Что касается собственных специалистов, то деятельность IT-армии быстро развилась от простого взлома российских веб-сайтов в первые дни вторжения до изощренных шпионских кампаний и первой подрывной кибератаки, направленной на гражданскую видеоплатформу, в начале мая 2022 года. Пока неясно, на каких кибероперациях группа собственных специалистов собирается сосредоточиться в будущем. Но, если судить по эволюционной траектории, которую мы наблюдаема последние 4 месяца, российские защитники, скорее всего, столкнутся с целым рядом экспериментальных кибероперациий, которые будут нацелены на все более и более серьезное воздействие и длительные последствия. Учитывая данную траекторию, особенно любопытно наблюдать, как группа юристов-правозащитников недавно решила подтолкнуть Международный уголовный суд в Гааге к возбуждению первого в истории дела о кибервойне против Sandworm – подразделения российской военной разведки, которое успешно атаковало предприятия электроэнергетики на Украине и вызвало короткие региональные отключения электроэнергии еще в 2015-2016 гг.[4]

Методика исследования

Ключевая задача подготовки настоящего отчета – представить всестороннее исследование, которое послужит основой для понимания, оценки и анализа поведения IT-армии и экосистемы, которая ее подпитывает.

Фактически, настоящий отчет составлен с использованием только общедоступных данных. Сюда входят общедоступные веб-сайты, сообщения в Twitter, статьи в СМИ, интервью, подкасты, видео на Youtube, формы GoogleDoc, а также сотни каналов и чатов Telegram. При проведении данного исследования автор никоим образом не участвовал ни в одной из вредоносных или незаконных кибератак, упомянутых в этом отчете.

Присоединение к сотням каналов и чатов Telegram, а также их чтение имело особое значение для получения доступа к детальной информации, содержащейся в настоящем отчете, и придания ей контекста. Например, функция поиска в Telegram позволяет исследователям просматривать каждый канал, на который они подписаны, и каждый чат, участником которого они являются. Данная функция была особенно полезна для отслеживания определенных терминов, целей, URL-адресов, IP-адресов и номеров портов в пределах нескольких каналов и чатов Telegram: Чем к большему количеству каналов и чатов вы присоединились, тем больше у вас обзор на данной платформе. Функция поиска также отображает поисковые запросы в хронологическом порядке, что значительно упрощает отслеживание информации до ее вероятного источника.

Обратите внимание на то, что присоединение к каналу, или чату Telegram не означает какого-либо официального членства и не налагает на автора никаких обязательств – финансовых, политических или иных.
Присоединение к каналу Telegram делает вас подписчиком, таким образом, например, позволяя настраивать оповещения о новых сообщениях. Вы также можете присоединиться к чату Telegram, что сделает вас участником этого чата, и даст возможность писать в чате. В то время как большинство каналов и чатов можно просматривать без регистрации, некоторые каналы и чаты не позволяют пользователям, не являющимся подписчиками или участниками, видеть их содержимое. Иногда, чтобы подписаться также требуется подтверждение администратора канала. Обычно оно предоставляется в течение нескольких минут и применяется только для осуществления ограниченной формы контроля доступа пользователей. В частности, российские хакерские группы используют этот процесс для избавления от проукраински настроенных пользователей.

В процессе настоящего исследования автор не размещал посты ни в одном из Telegram-каналов или чатов. Он также не вступал в какие-либо частные беседы с пользователями Telegram в огромном множестве каналов и чатов. Автор беседовал с несколькими хакерскими группами в Twitter, которые утверждали, что сотрудничают с IT-армией. Тем не менее, ни одно из этих утверждений не могло быть подтверждено – и впоследствии соответствующая информация не была включена в этот отчет – поскольку IT-армия не реагировала на запросы автора по электронной почте.

Относительно ограничений данного отчета необходимо подчеркнуть два момента. Во-первых, автор не ознакомился абсолютно со всеми соответствующими хакерскими сообществами в Telegram, поскольку он, вероятно, не стал участником каждого соответствующего канала или чата Telegram. Таким образом, нет полной ясности, имели ли место в Telegram какие-либо другие информационные потоки, которые не удалось зафиксировать при подготовке данного отчета. Во-вторых, к просмотру определенных сообщений в чатах Telegram обычным образом подключиться невозможно, а доступ к довольно большому количеству чатов предоставляется через публичные приглашения с ограниченным временем действия. Как итог,

[2] Журнал «Одесса», «Украина получила две награды в области кибербезопасности на Европейском форуме кибербезопасности CYBERSEC», Журнал «Одесса», 18 мая 2022 г., https://web.archive.org/web/20220608141159/https://odessa-journal.com/ukraine-received-two-awards-in-the-field-of-cybersecurity-at-the-cybersec-european-cybersecurity-forum/.

[3] Там же.

[4] Энди Гринберг, «Дело по обвинению в военных преступлениях против российских хакеров Sandworm», *Wired*, 12 мая 2022 г., https://www.wired.com/story/cyber-war-crimes-sandworm-russia-ukraine/.

в настоящем отчете не представляется возможным указать актуальные URL-адреса для большинства чатов, а также конкретные URL-адреса для ссылок на отдельные сообщения в чате Telegram. Везде, где это возможно, ссылки на телеграммы заархивированы с помощью archive[.]ph, а ссылки, не относящиеся к Telegram, заархивированы с помощью Wayback Machine.

2 Возникновение

Создание IT-армии Украины начато Егором Аушевым. Аушев – известный украинский ИТ-предприниматель и соучредитель трех компаний, деятельность которых стала все более актуальной в условиях восьмилетней войны с Россией – Cyber Unit Tech, Cyber School и Hacken.io. Где-то между 24 февраля (днем российского вторжения) и 26 февраля Аушев предложил идею добровольческой киберармии Михаилу Федорову, молодому 31-летнему министру цифровой трансформации Украины.[5]

Примерно в то же время, по просьбе высокопоставленного чиновника Министерства обороны Украины, Аушев также приступил к созданию украинской добровольческой группы кибербезопасности численностью 1000 человек.[6] Для этого Аушев распространял соответствующую информацию в Twitter и на различных форумах, посвященных хакерству, разместив форму заявки в Google Docs, чтобы с ее помощью оценить уровень квалификации и область знаний кандидата.[7] По мнению Аушева, эта группа из примерно 1000 украинских добровольцев – специалистов по кибербезопасности должна быть разделена на наступательную и защитную группы. В беседе с агентством Reuters 24 февраля Аушев уточнил, что оборонительная группа будет «задействована для защиты инфраструктуры, такой как электростанции и системы водоснабжения», а наступательная группа будет помогать «украинским военным проводить операции цифрового шпионажа против вторгающихся российских сил». Как выразился Аушев, «на территории нашей страны находится армия. [...] Нам нужно знать, что они делают».[8] На момент написания данной статьи соотношение между этими двумя группами все еще неизвестно.

Вдохновленный идеей Аушева о добровольческой киберармии, Федоров зашел в Facebook 26 февраля в 9.00 утра по центральноевропейскому времени (CET) и разместил следующий пост на украинском языке: «У нас много талантливых украинцев в цифровой сфере: разработчики, киберспециалисты, дизайнеры, копирайтеры, маркетологи, таргетологи и т.д. Мы создаем IT-армию. Все оперативные задачи будут представлены в Telegram-канале: t.me/itarmyofurraine. Найдется задача для каждого».[9] Это же сообщение на украинском языке Федоров опубликовал в своем верифицированном Telegram-канале, насчитывающем 170 000 подписчиков.[10] А в 19.38 по центральноевропейскому времени (CET) в его верифицированном аккаунте Twitter появилось сообщение на английском языке: «Мы создаем IT-армию. Нам нужны талантливые люди из цифровой отрасли. Все оперативные задачи будут представлены здесь: t.me/itarmyofurraine».[11]

Освещение западными СМИ рождения IT-армии было почти исключительно сосредоточено на посте Федорова в Twitter, поскольку он был написан на английском языке, при этом его посты в Facebook и Telegram были проигнорированы.[12] Но между этими тремя постами есть любопытные различия. Во-первых, целевая аудитория Федорова в Twitter была явно международной, в то время как сообщение в Facebook и Telegram было адресовано, в первую очередь, украинцам. Во-вторых, в своих постах в Facebook и Telegram Федоров очень точно описал, какие именно таланты нужны IT-армии. В–третьих, во всех трех сообщениях Федоров неправильно написал слово «украина», при этом позже был исправлен только его пост в Telegram. Забавно, что из-за этой ошибки есть только один пост на канале «itarmyofurraine», который перенаправляет пользователей на официальный и правильный канал «itarmyukraine2022». Любопытно, что в тот же день кто-то также решил открыть Telegram-канал под названием «itarmyofuraine» (одна буква «r», отсутствует буква «k»), который в настоящее время насчитывает около 11 500 подписчиков и репостит часть контента с официального канала.[13] Пожалуй, важнее всего, что западные СМИ не заметили сообщение официального Telegram-канала Министерства цифровых преобразований от 26 февраля в 18:48 по центральноевропейскому времени. Его содержание было почти идентично мобилизационному сообщению Федорова, за исключением того, что министерство добавило одну важную фразу: «Мы призываем вас использовать любые векторы кибератак и DDoS-атак на российские ресурсы».[14] Этот призыв к оружию

[5] См. также: Адам Янофски, «Эта украинская киберфирма предлагает хакерам вознаграждение за обрушение российских сайтов», веб-ресурс *The Record*, 4 марта 2022 года, https://web.archive.org/web/20220608141213/https://therecord.media/this-ukrainian-cyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites/.

[6] Джоэл Шектман и Кристофер Бинг, «ЭКСКЛЮЗИВ! Украина призывает хакерские сообщества вести оборонительную деятельность против России», *Reuters*, 24 февраля 2022 г., https://web.archive.org/web/20220608141232/https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/.

[7] Грэм Клули, «Украина ищет хакеров-добровольцев для защиты своей критической инфраструктуры и слежки за российскими войсками», *Bitdefender*, 25 февраля 2022 г., https://web.archive.org/web/20220608141452/https://www.bitdefender.com/blog/hotforsecurity/ukraine-calls-for-volunteer-hackers-to-protect-its-critical-infrastructure-and-spy-on-russian-forces/.

[8] Джоэл Шектман и Кристофер Бинг, «ЭКСКЛЮЗИВ! Украина призывает хакерские сообщества вести оборонительную деятельность против России», *Reuters*, 24 февраля 2022 г., https://web.archive.org/web/20220608141232/https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/.

[9] Михаил Федоров, Facebook, 26 февраля 2022 г., https://www.facebook.com/mykhailofedorov.com.ua/posts/1005386320078887.

[10] Михаил Федоров, Telegram-канал, 26 февраля 2022 г., https://t.me/zed- igital/1114 или https://archive.ph/H2caw.

[11] Михаил Федоров, Twitter, 26 февраля 2022 г., https://web.archive.org/web/20220226232059/https://twitter.com/FedorovMykhailo/status/1497642156076511233.

[12] Например, *Wired*, ссылка на пост Федорова в Facebook, см.: Том Саймонайт и Джан М. Вольпичелли, «Минцифры Украины – это грозная военная машина», *Wired*, 17 марта 2022 г., https://www.wired.com/story/ukraine-digital-ministry-war/.

[13] Описание как официального канала IT-армии, так и itarmyofuraine включает официальную электронную почту IT-армии Украины (itarmyua@gmail.com).

[14] Министерство цифровой трансформации, Telegram-канал, 26 февраля 2022 г., https://t.me/mintsyfra/2609 или https://archive.ph/7UYkx.

повторял самый первый пост в официальном Telegram-канале IT-армии, который был опубликован двумя часами ранее: «Задача № 1 Мы призываем вас использовать любые векторы кибератак и DDoS-атак на данные ресурсы». Далее в посте были перечислены адреса веб-сайтов, всего 31 адрес: российские банки, коммерческие организации и правительственные сайты.[15]

На момент написания настоящей статьи неизвестно, что именно вызвало резкий внутренний сдвиг от объединения вместе разработчиков, дизайнеров и копирайтеров к практически единственной задаче для IT-армии – сфокусироваться на DDoS-атаках. Одно из возможных пояснений состоит в том, что украинские специалисты по конкретным направлениям, которые Федоров упомянул в своем посте, в конце концов был направлены в группу под названием «StandForUkraine». Группа StandForUkraine поддерживается Романом Захаровым, 37-летним украинским главой ИТ-компании. В настоящее время в группу входят около 1300 «инженеров-программистов, менеджеров по маркетингу, графических дизайнеров и покупателей онлайн-рекламы», которые сражаются на фронте информационной войны Украины.[16] Группа пытается мобилизовать не только украинцев, но и международное сообщество против российского вторжения и распространяет украинскую военную пропаганду через западные СМИ и платформы социальных сетей. Группа также способствовала уходу западных компаний из России.[17] StandForUkraine имеет свой собственный веб-сайт, но, в отличие от IT-армии, для общения и решения организационных вопросов в ней используются только приватные чаты по приглашению в приложении для обмена сообщениями Signal. Более подробно экосистема StandForUkraine может быть проанализирована в будущих исследованиях CSS.

Что касается IT-армии, то важно подчеркнуть, что Федоров очень активен в Telegram, но с ноября 2020 года опубликовал в Twitter всего около 500 сообщений. При этом даже в Telegram Федоров редко говорит об IT-армии. В период с 26 февраля по 20 апреля он перепостил только 18 сообщений с официального канала IT-армии. Для министра, создавшего эту цифровую армию добровольцев, Федоров, похоже, не очень-то и интересуется данным вопросом. Вместо этого большинство его сообщений в Telegram посвящены его усилиям по призывам к западным компаниям уйти из России, сбору средств на гуманитарные проекты и вооруженные силы Украины, а также информированию граждан о работе возглавляемого им Министерства.

Логично было бы предположить, что веб-сайт Министерства цифровой трансформации будет наглядно демонстрировать свою связь с IT-армией и каким-то образом, в той или иной форме освещать его текущую деятельность.[18] Но это не так. На момент написания этой статьи на веб-сайте министерства нет ни одной новости, в которой говорилось бы об IT-армии. Аналогичным образом, официальный Telegram-канал Министерства упомянул IT-армию всего десять раз и перепостил всего четыре сообщения с официального канала IT-армии в период с 26 февраля по 20 апреля.[19] Возможно, реагируя на информацию об отсутствии последовательного освещения, 18 апреля Telegram-канал Министерства объявил, что в дальнейшем каждый понедельник он будет рассказывать о победах IT-армии.[20] Примечательно, что 23 мая Министерство резюмировало, что «с момента российского вторжения на Украину IT-армия атаковала около 2000 российских ресурсов».[21]

Любопытно, что министерство действительно упомянуло IT-армию и ее Telegram-канал в двух новостях на kmu.gov.ua – официальном веб-портале украинского правительства – более чем через две недели после мобилизационного призыва Федорова. В новостном сообщении от 10 марта кратко признавалось существование IT-армии, в то время как сообщение от 12 марта было озаглавлено: «Министерство цифровой трансформации создало 3 службы для борьбы с оккупантами на цифровом фронте»: IT-армия, Интернет-силы Украины и приложение e-Enemy «еВорог».[22]

Неравномерное и несколько хаотичное освещение деятельности IT-армии Министерством цифровой трансформации в первые два месяца после вторжения может быть результатом размытой и все еще развивающейся организационной структуры самой IT-армии.

Сколько человек в составе IT-армии?

Согласно публичным отчетам, число членов IT-армии составляет около 300 000 человек, что сопоставимо с количеством подписчиков официального Telegram-канала IT-армии.[23] По данным TGStat – платформы, которая предоставляет аналитику по каналам и чатам Telegram,

[15] IT-армия Украины, Telegram-канал, 26 февраля 2022 года, https://t.me/itarmyofukraine2022/1 или https://archive.ph/SMt31.

[16] Фрэнк Баяк, «Цифровая армия Украины наращивает кибератаки, разведывательную и информационную войны», Ассошиэйтед Пресс (Associated Press), 5 марта 2022 г., https://web.archive.org/web/20220608141931/https://apnews.com/article/russia-ukraine-technology-europe-hacking-f2c4960e48b8022a567780f3602b54e2.

[17] Там же.

[18] Веб-сайт Министерства цифровой трансформации Украины, https://thedigital.gov.ua/; Telegram-канал Министерства цифровой трансформации, https://t.me/mintsyfra.

[19] Министерство цифровой трансформации, Telegram-канал, поисковые запросы «IT Army» и «IT-армію», https://t.me/s/mintsyfra?q=%D0%86%D0%A2-%D0%B0%D1%80%D0%BC%D1%96%D1%8E; https://t.me/s/mintsyfra?q=it+army.

[20] Министерство цифровой трансформации, Telegram-канал, 18 апреля 2022 г., https://t.me/mintsyfra/2921 или https://archive.ph/rDwiT.

[21] Министерство цифровой трансформации, Telegram-канал, 23 мая 2022 г., https://t.me/mintsyfra/3065 или https://archive.ph/qJk5P.

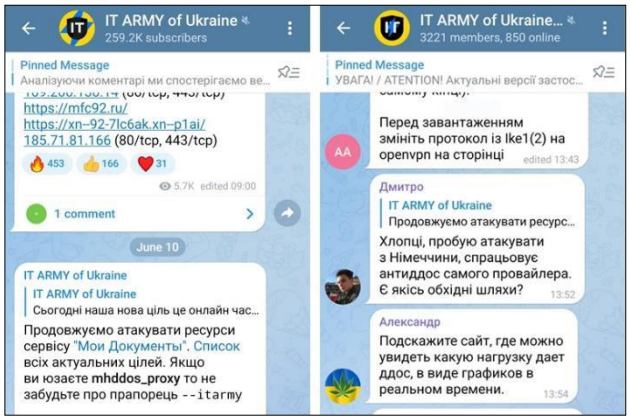
[22] KMU.gov.ua, «Мінцифри бореться з ворогом на цифровому фронті», 10 марта 2022 года, https://web.archive.org/web/20220310141242/https://www.kmu.gov.ua/news/mincifri- boretsya-z-vorogom-na-cifrovomu-fronti; KMU.gov.ua, «Мінцифри створило 3 сервіси, щоб боротися з окупантами на цифровому фронті», 12 марта 2022 года, https://web.archive.org/web/20220313185053/https://www.kmu.gov.ua/news/mincifri- stvorilo-3-servisi-shchob-borotisya-z-okupantami-na-cifrovomu-fronti.

[23] Крис Стокел-Уокер и Дэн Милмо, «Именно так и надо делать: 300 000 хакеров-добровольцев объединяются для борьбы с Россией», The Guardian, 15 марта 2022 г., https://web.archive.org/web/20220608145557/https://www.theguardian.com/world/2022/mar/15/volunteer-hackers-fight-russia; Корин Файф, «На Украине хактивисты борются с утечками данных», ресурс *The Verge*, 11 марта 2022 года, https://web.archive.org/web/20220608145521/https://www.thev-

– Telegram-канал IT-армии имел максимальное количество подписчиков 26 марта, а именно 307 165 человек.[24] С тех пор цифры постоянно снижались, что привело к совокупной потере 47 940 подписчиков в течение следующих восьми недель (15,6%). На 10 июня количество подписчиков IT-армии составило 259 225 человек.[25]

Хотя неизвестно, по какой именно причине канал так быстро теряет подписчиков, наиболее вероятным объяснением, по всей видимости, является сочетание следующих моментов (1) потеря новизны с течением времени, (2) скука из-за повторяющихся задач и (3) продолжающаяся реальная война, на которую DDoS-атаки IT-армии, целью которых в основном является российская гражданская инфраструктура, значительного влияния не оказывают.

Чтобы точнее оценить количество подписчиков IT-армии, полезно знать, что Telegram предлагает два типа платформ: (а) каналы, в которых отображаются только сообщения администратора канала, а пользователи могут размещать комментарии, если эта функция включена. И (б) чаты, в которых пользователи действительно могут вести своего рода диалог с несколькими участниками.



10 июня 2022 г., скриншоты канала (слева) и чата (справа) IT-армии

В Telegram-канале IT-армии, который открыт, буквально, для всех, практически не проводится глубоких оперативных обсуждений. У IT-армии также есть официальный чат в Telegram, однако его численность составляет всего 3 200 человек. Обсуждение в чате в первую очередь направлено на то, чтобы помочь другим участникам решить их технические проблемы и время от времени определить новые потенциальные российские цели для DDoS-атак.

Итак, сколько же человек в действительности входит в IT-армию? На самом деле никто не знает, даже сама IT-армия. Что IT-армия знает, или, точнее говоря, что известно координационной группе IT-армии и администраторам Telegram-каналов, так это точное количество людей, которые напрямую обратились к ним, чтобы предложить свои навыки и время через учетную запись Gmail IT-армии и контактные формы Google Docs.[26] На момент написания этой статьи это число не было публично раскрыто.

3 Определение целей и координация

Что мы знаем точно, так это то, что Telegram-канал IT-армии является лишь одним из компонентов организационной структуры IT-армии – по сути, он служит своего рода мегафоном для распространения информации о целях DDoS-атак.[27] В интервью украинскому изданию Media Sapiens в конце марта Мстислав Баник, руководитель отдела развития электронных сервисов Министерства цифровой трансформации, пояснил, что «все задачи формируются кураторами канала, которые распределяют их в канале для волонтеров. Любой желающий может подписаться на Telegram-канал проекта и получать задания».[28]
Ниже на примере нескольких фактических ситуаций мы поясним, как видимая часть этого определения целей работает на практике.

Простая постановка задачи

Первый пример касается «простой постановки задач». В данном случае одна и та же информация о целях атаки, которую публикует канал IT-армии, распространяется во множестве других каналов и чатов. В 15:50 18 марта по центральноевропейскому времени (CET) канал IT-армии разместил пост со следующей информацией:

erge.com/2022/3/11/22968049/anonymous-hacks-ukraine-russia-cybercrime-danger; Элиз Лабот, ««Мы первые в мире, кто стал использовать это новое оружие: Цифровая битва Украины против России"», *Politico*, 8 марта 2022 года, https://web.archive.org/web/20220608135145/https://www.polit-ico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber- social-media-00014880.

[24] TGStat, «IT-армия Украины – количество подписчиков растет», дата не указана, https://tgstat.com/channel/@itarmyofukraine2022/stat/subscribers.

[25] Там же.

[26] IT-армия, «IT Army», Google Docs, дата обращения – март или апрель, https://web.archive.org/web/20220509133343/https://docs.google.com/forms/d/e/1FAIpQLSfeFKKXQkQaZDwVPZQVRSvbETYtsVZXBawF7fawHeC-m4mQZw/view-form; IT-армия, «Предложить помощь», Google Docs, дата обращения – март или апрель, https://web.archive.org/web/20220509133603/https://docs.google.com/forms/d/e/1FAIpQLSe3M1jW5ieBkd4FMpktrFuRpCpmF5zQjg8W1qHe9uO0z_QO-g/viewform

[27] Относительно оценки воздействия DDoS-атак см.: Крис Партридж, «ru- ok», веб-сервис Github, https://web.archive.org/web/20220608112818/https://github.com/tweedge/ru-ok; Кайл Алспач, «Украинская IT-армия успешно наносит по России удары, которые приводят к издержкам и хаосу», *VentureBeat*, 4 марта 2022 года, https://web.archive.org/web/20220608145845/https://venturebeat.com/2022/03/04/ukraines-it-army-is-doing-well-hitting-russia-with-cost-and-chaos/.

[28] Ира Рябоштан, «Мстислав Банік, Мінцифри: Західні компанії не мають ставати спонсорами російського вторгнення та загибелі українців», *Media Sapens*, 23 марта 2022 года, https://web.archive.org/web/20220608112712/https://ms.detector.media/internet/post/29223/2022-03-23-mstyslav-banik-mintsyfry-zakhidni-kompanii-ne-mayut-stavaty-sponsoramy-rosiyskogo-vtorgnennya-ta-zagybeli-ukraintsiv/.

URL-адрес vesti95[.]ru, один из IP-адресов vesti95 и четыре порта. *Vesti95 (Вести Республики)* – официальная газета, издаваемая Министерством Чеченской Республики по национальной политике, внешним связям, печати и информации. Всего через три минуты та же информация появилась в чате под названием «DDoS Joint Group» («Объединенная группа DDoS-атак») (около 1900 участников). Через 20 минут после этого она также была опубликован на канале «Hacker Forces» (около 1100 подписчиков), который является официальным каналом добровольческой киберармии Hacken.io. Hacker Forces указали источник информации, объяснив это так: «вот новое задание от itarmyofukraine2022. Вы с нами?»[29] В 17:39 канал под названием «Studentcyberarmy» (около 900 подписчиков) опубликовал точно такую же информацию, не ссылаясь на IT-армию и, буквально в ту же минуту, эта информация была перепощена в чате «CyberFire» (около 5500 подписчиков).[30] В 19:00 канал, принадлежащий «Cyber Palyanitsa» (около 700 подписчиков), опубликовал те же данные о цели без указания ссылки на источник.[31] А в 19:59 по центральноевропейскому времени (CET) информация появилась на канале «disBalancer Ukraine» (около 5500 подписчиков), который является инструментом DDoS-атак украинского канала Hacken.io.[32] В 16.16 20 марта по центральноевропейскому времени (CET) канал «disBalancer English» (около 13 500 подписчиков) разместил URL-адрес vesti[.]ru под заголовком «Сайты, [которые] подверглись атаке 18 марта 2022 года».[33] Час спустя это сообщение было перепощено каналом Hacker Forces.[34] На данном примере видно, что Hacken.io глубоко интегрирован в информационный поток, исходящий из канала IT-армии. Это не удивительно с учетом того, что Аушев был соучредителем Hacken.io. На самом деле взаимосвязь между IT-армией и Hacken.io гораздо глубже, более подробнее об этом расскажем позже.

Дата и время	Канал или чат	Раскрытая информация о целях атаки
18 марта 15:50	канал IT-Армии Украины	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
18 марта 15:50	чат IT-Армии Украины	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
18 марта 16:13	канал Hacker Forces	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
18 марта 17:39	канал Studentcyberarmy	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
18 марта 17:39	чат CyberFire	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
18 марта 19:00	Канал Cyber Palyanitsa	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
18 марта 19:59	канал disBalancer Ukraine	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
20 марта 16:16	канал disBalancer	Vesti95.ru
20 марта 17:16	канал Hacker Forces	Vesti95.ru

Дополнение информации о цели атаки

Второй пример посвящен тому, что можно описать, как «дополнение информации о цели атаки». Информация о цели атаки, размещенная каналом IT-армии, распространяется только при условии ее дополнения все новыми IP-адресами и портами. В 9:11 утра 14 марта по центральноевропейскому времени (CET) канал IT-армии разместил url-адрес asna[.]ru и один из IP-адресов данного сайта. Компания Asna представляет сеть из более чем 10 000 аптек в России, а ее веб-сайт функционирует как федеральная онлайн-аптека. Информацию о цели атаки перепостили только в чате «DDoS Joint Group» и на канале под названием «KiberBull» (около 7800 подписчиков), больше она не появилась ни в одном из доступных мне каналов или чатов.[35] Расклад изменился восемь дней спустя, когда 22 марта в 10:38 утра по центральноевропейскому времени (CET) канал Studentcyberarmy объявил: «Доброе утро, сегодня мы начинаем наш день на киберфронте с магазина фармацевтической отрасли, а именно ASNA! Атака продлится до 13:00!»[36] В данный пост был включен IP-адрес, упомянутый IT-армией, два дополнительных целевых IP-адреса и шесть портов – по два для каждого из трех IP-адресов. Через одну минуту данный пост был перепощен чатами CyberFire и «DDoS Attack Cyber Cossacks» (около 25 800 участников). В 10:51 утра по центральноевропейскому времени (CET), чат «Cyber Cerber» (около 600 участников) опубликовал точно такую же информацию о цели атаки, не ссылаясь на источник, а в 11:35 канал «DDoS Attack Cyber Cossacks» (около 69 800 подписчиков) дал задание DDoS-группам №№ 1 и 4 нанести удар по трем IP-адресам Asna. Каждая группа Cyber Cossacks DDoS включает примерно 1000 специалистов, которые очень активны и координируют свои действия в своих отдельных чатах. На следующий день, в 12:08 по центральноевропейскому времени (CET) Cyber Palyanitsa снова опубликовала эту же информацию по цели атаки. Девять минут спустя она появилось в чате Cyber Cerber, а через восемь минут был репост на канале под названием «Anonymous-Ukraine» (около 1900 подписчиков).[37] Ровно в 12:29 по центральноевропейскому времени (CET) канал Studentcyberarmy опубликовал новый пост с той же информацией об атаке на Asna, который был немедленно перепощен чатом CyberFire. Семь минут спустя канал DDoS Attack Cyber Cossacks опубликовал команды для извлечения самого последнего Docker image («докерного образа»), чтобы обновить информацию об атаке на

[29] Hacker Forces, Telegram-канал, 18 марта 2022 года, https://t.me/hackencyberarmy/101 или https://archive.ph/ILjlY.

[30] Studentcyberarmy, Telegram-канал, 18 марта 2022 года, https://t.me/student-cyberarmy/193 или https://archive.ph/mfXYH; CyberFire Chat, Telegram-канал, 18 марта 2022 года, https://t.me/cyberfirechatt/52321 или https://archive.ph/niCZo.

[31] CyberPalyanitsa, Telegram-канал, 18 марта 2022 года, https://t.me/CyberPal-yanitsa/215 или https://archive.ph/ZKCBq.

[32] disBalancer Ukraine, Telegram-чат, 18 марта 2022 года, https://t.me/c/1701910482/50239.

[33] disBalancer English (английский), Telegram-канал, 20 марта 2022 года, https://t.me/disbalancer_group/113188 или https://archive.ph/dBWON.

[34] Hacker Forces, Telegram-канал, 20 марта 2022 года, https://t.me/hackencyberarmy/108 или https://archive.ph/P3WqP.

[35] KiberBull, Telegram-чат, 14 марта 2022 года, https://t.me/c/1549333360/346.

[36] Studentcyberarmy, Telegram-канал, 22 марта 2022 года, https://t.me/student-cyberarmy/209 или https://archive.ph/DnK1M.

[37] Anonymous-Ukraine, Telegram-канал, 23 марта 2022 года, https://t.me/ciberwars/740 или https://archive.ph/ShKfQ.

asna[.]ru.[38] Во всем этом информационном обмене обращает на себя внимание отсутствие Hacken.io.

Дата и время	Канал или чат	Раскрытая информации о целях атаки
14 марта 09:11	канал IT-Армии Украины	178.248.235.156
14 марта 09:11	чат IT-Армии Украины	178.248.235.156
22 марта 10:38	канал Studentcyberarmy	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
22 марта 10:39	чат CyberFire	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
22 марта 10:39	чат DDoS Attack Cyber Cossacks	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
22 марта 10:51	канал Cyber Cerber	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
22 марта 11:35	канал DDoS Attack Cyber Cossacks	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
23 марта 12:08	канал Cyber Palyanitsa	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
23 марта 12:17	канал Cyber Cerber	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
23 марта 12:25	канал Anonymous Ukraine	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
23 марта 12:29	канал Studentcyberarmy	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
23 марта 12:29	чат CyberFire	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
23 марта 12:36	канал DDoS Attack Cyber Cossacks	docker run -it --rm --pull always ghcr.io/porthole-as- cend-cinnamon/mhddos_proxy:latest http://www.asna.ru/ -t 1500 --rpc 1000 -p 1000 -- http-methods STRESS –debug MHDDoS: python start.py STRESS http://www.asna.ru/ 5 1000 proxy.txt 100 3600 true

Внешняя кластеризация

Третий пример – это «внешняя кластеризация», при которой информация о целях атаки не получает широкого распространения, а сохраняется только в небольшой группе каналов и чатов. 28 февраля и 3 марта URL-адрес mvideo[.]ru был упомянут в чатах disBalancer Ukraine и CyberFire. «М.Видео» – одна из крупнейших сетей бытовой электроники в России. Призыв атаковать «М.Видео» не был подхвачен никем до тех пор, пока две недели спустя Cyber Palyanitsa не опубликовала 3 IP-адреса и 18 разных портов «М.Видео» в 21:19 по центральноевропейскому времени. Одиннадцать минут спустя канал Studentcyberarmy опубликовал ту же самую информацию о цели атаки, и буквально в течение одной минуты сообщение было перепощено чатом CyberFire. В 22:21 данную информацию также подхватил Cyber Cerber. Наконец, 7 мая «М.Видео» в качестве цели своей DDoS-атаки провозгласила IT-армия, при этом дублировался один из IP-адресов, указанный в ранее представленной информации.[39] Группа, известная как «Украинский жнец» (Ukrainian Reaper), опубликовала команды для обновления скрипта Multiddos посредством docker и MHDDoS с использованием Python.[40]

Примечание: Multiddos – это DDoS-скрипт, который используется исключительно «Украинским жнецом». Он объединяет в себе три инструмента: auto_mhddos, разработанный «Украинским жнецом», db1000n и UA Cyber Shield.[41] Два последних мы обсудим в следующем разделе.

Дата и время	Канал или чат	Раскрытая информации о целях атаки
28 февраля, 08:20	чат disBalancer Ukraine	mvideo.ru
3 марта 15:53	чат CyberFire	mvideo.ru
19 марта 21:19	канал Cyber Palyanitsa	185.71.67.88 (80/http, 443/HTTP); 5.188.118.38 (22/SSH, 80/http, 123/NTP, 443/HTTP, 3306/MYSQL, 44060/Unknown); 37.140.192.237 (21/FTP, 22/SSH, 25/SMTP, 53/DNS, 80/HTTP, 110/POP3, 111/PORTMAP, 143/IMAP, 3306/MYSQL)
19 марта 21:30	канал Studentcyberarmy	185.71.67.88 (80/http, 443/HTTP); 5.188.118.38 (22/SSH, 80/http, 123/NTP, 443/HTTP, 3306/MYSQL, 44060/Unknown); 37.140.192.237 (21/FTP, 22/SSH, 25/SMTP, 53/DNS, 80/HTTP, 110/POP3, 111/PORTMAP, 143/IMAP, 3306/MYSQL)
19 марта 21:30	чат CyberFire	185.71.67.88 (80/http, 443/HTTP); 5.188.118.38 (22/SSH, 80/http, 123/NTP, 443/HTTP, 3306/MYSQL, 44060/Unknown); 37.140.192.237 (21/FTP, 22/SSH, 25/SMTP, 53/DNS, 80/HTTP, 110/POP3, 111/PORTMAP, 143/IMAP, 3306/MYSQL)
19 марта 22:21	канал Cyber Cerber	185.71.67.88 (80/http, 443/HTTP); 5.188.118.38 (22/SSH, 80/http, 123/NTP, 443/HTTP, 3306/MYSQL, 44060/Unknown); 37.140.192.237 (21/FTP, 22/SSH, 25/SMTP, 53/DNS, 80/HTTP, 110/POP3, 111/PORTMAP, 143/IMAP, 3306/MYSQL)
7 мая, 08:00	канал IT-Армии Украины	mvideo.ru/tehnika-dylya-kuhni 185.71.67.88 (80/TCP, 44/TCP) api.mvideo.ru webapi.mvideo.ru 185.71.67.88 (80/TCP, 443/TCP)
7 мая 10:29	Украинский жнец	multiddos (Layer 4 + 7) docker run -it --rm --log-driver none --name multidd --pull always karboduck/multidd mhddos_proxy (Layer 4 +7): python3 runner.py --itarmy --http-methods GET STRESS -t 250

Ситуативная приоритизация

Четвертый пример иллюстрирует то, что было бы уместно обозначить, как «ситуативная приоритизация». В данном случае отдельные фрагменты информации о цели атаки всплывают в разных каналах и чатах, но объединяются только гораздо позже, когда IT-армия присваивает цели высокий приоритет. В период с 28 февраля по 4 марта атака на qiwi[.]com широко обсуждалось в чате IT-армии, чате CyberFire, а также двух чатах disBalancer. QIWI – популярный российский поставщик платежных услуг, который также обслуживает другие страны Содружества Независимых Государств (СНГ). Многие пользователи Telegram спрашивали, почему QIWI не был объявлен целью DDoS-атаки. Один из пользователей, например, пошутил, что QIWI не следует использовать в качестве цели атаки, потому что должен оставаться хотя бы один способ отправки денег из России на Украину. Другие просто заявляли, что они сейчас

[38] DDoS Attack Cyber Cossacks, Telegram-канал, 23 марта 2022 года, https://t.me/ddos_separ/903 или https://archive.ph/584td.

[39] IT-армия Украины, Telegram-канал, 7 мая 2022 года, https://t.me/itarmyofukraine2022/331 или https://archive.ph/QkT15.

[40] Украинский жнец, Telegram-канал, 7 мая 2022 года, https://t.me/ukrainian_reaper_ddos/244 или https://archive.ph/fYerr.

[41] https://web.archive.org/web/20220608113119/https://github.com/KarboDuck/multiddos/blob/main/README.md. См. также: Украинский жнец, «Украинский жнец на связи. DDOS-им РФ с помощью Multiddos», *Mezha (Межа)*, 21 мая 2022 года, https://web.archive.org/web/20220608104948/https://mezha.me- dia/articles/ddos-rf-z-multiddos/.

проводят DDoS-атаки на QIWI в индивидуальном порядке.

Динамика изменилась 4 марта, когда QIWI опубликовала заявление для прессы, в котором отмечалось, что «санкции США и ЕС в отношении России не оказали непосредственного и существенного влияния на деятельность QIWI. Ни QIWI, ни какая-либо из ее дочерних компаний конкретно не подпадают под новые санкции, введенные в результате российских военных операций на Украине».[42] В тот же день канал «DDoS Attack Cyber Cossacks» (около 69 800 подписчиков) объявил об атаке на QIWI и опубликовал один IP-адрес и два порта.[43] Несколько часов спустя был опубликован новый пост, в котором цель была изменена на другой IP-адрес QIWI с пометкой: «Давайте попробуем подключить больше людей, начнем в 9:23, атакуйте до тех пор, пока я не дам новую цель».[44] Обсуждение атаки на QIWI продолжалось в течение следующих 25 дней, когда различные каналы и чаты публиковали другие IP-адреса QIWI и проводили собственные DDOS-атаки. Затем, 29 марта, канал IT-армии неожиданно объявил, что «нам необходимо атаковать QIWI прямо сейчас».[45] В посте было перечислено 15 IP-адресов и портов QIWI, включая все те, которые ранее уже были распространены в различных каналах и чатах. По какой-то причине в тот же день IT-армия решила объявить QIWI высокоприоритетной целью DDoS-атаки, то есть систему предлагалось обрушить немедленно.

Примечательно, что ситуативная приоритизация также была применена при организации атаки IT-армии на ЕГАИС в начале мая 2022 года. ЕГАИС – это единая государственная автоматизированная информационная система для отслеживания оборота алкогольной и спиртосодержащей продукции, внедренная российским правительством. Она представляет собой централизованную систему, учитывающую сертификацию и налогообложение в разрезе каждой бутылки алкоголя, водки, или вина, произведенных в России. Еще в начале апреля 2022 года один из пользователей в чате IT-армии трижды упоминал ЕГАИС как хорошую цель для DDoS-атак. Как пояснил сам пользователь 4 апреля: «Поверьте мне, эта цель довольно серьезна, потому что здесь имеет место репутационный ущерб. Данный портал принадлежит государству, и в соответствии с законодательством Российской Федерации магазины и дистрибьюторы должны обязательно дождаться оформления документов на этом портале».[46]
2 мая в 8:00 утра ЕГАИС была выбрана DDoS Attack Cyber Cossacks в качестве цели.[47] А в 8:55 канал IT-армии объявил, что «сегодняшнюю цель мы получили от одного из наших подписчиков. ЕГАИС – это российская федеральная государственная автоматическая система отслеживания производства и распространения алкогольных напитков в стране. Если эта система рухнет, официальный оборот спиртных напитков в России будет заблокирован!»[48]

По данным российского издания «Ведомости», «производители и дистрибьюторы алкоголя на первые майские праздники не смогли отгрузить продукцию своим покупателям из-за масштабного сбоя в работе [ЕГАИС]».[49] На период со 2 по 12 мая IT-армия обозначила ЕГАИС целью с высоким приоритетом. Например, 7 мая канал IT-армии сообщил, что «сегодня онлайн покупки в России будут отменены ;) И не забудьте продолжить работу с «ЕГАИС».[50] Аналогично, 8 мая канал пояснил: «у нас традиция бороться с русской пропагандой по воскресеньям. Не будем отступать от нее. Кроме того, мы хотели бы продолжать атаки на «ЕГАИС», ведь благодаря вашей помощи идет постоянный поток жалоб на этот сервис».[51]

По данным Министерства иностранных дел России, «по состоянию на май 2022 года более 65 000 «диванных хакеров» из США, Турции, Грузии и стран ЕС регулярно принимали участие в скоординированных DDoS-атаках на [российскую] критически важную информационную инфраструктуру».[52]

Координационный документ IT-армии

Теперь, когда у нас есть представление о том, как работает видимый обмен информацией о DDoS-атаках в Telegram, давайте взглянем на общедоступный координационный документ IT-армии, размещенный в Google Docs и доступный в официальном Telegram-боте IT-армии.[53] Для написания настоящего обзора использовалась версия, актуальная по состоянию на 30 марта.

Координационный документ периодически обновляется IT-армией и включает информацию о приоритетности целей DDoS-атак. Он также в общих чертах отслеживает, какие веб-сайты не работают, или нуждаются в повторном подключении, а также служит источником нескольких инструкций по инструментам DDoS в качестве рекомендаций

[42] QIWI, «QIWI заявляет, что ее оперативная деятельность проходит штатно», 4 марта 2022 года, https://web.archive.org/web/20220608113203/https://investor.qiwi.com/news-and-events/press-releases/3994532231/.

[43] DDoS Attack Cyber Cossacks, Telegram-канал, 4 марта 2022 года, https://t.me/ddos_separ/482 или https://archive.ph/Sqd3t.

[44] DDoS Attack Cyber Cossacks, Telegram-канал, 4 марта 2022 года, https://t.me/ddos_separ/495 или https://archive.ph/i6dtw.

[45] IT-армия Украины, Telegram-канал, 29 марта 2022 года, https://t.me/itarmyofukraine2022/247 или https://archive.ph/x0cHA.

[46] IT-армия Украины, Telegram-чат, 4 апреля 2022 года.

[47] DDoS Attack Cyber Cossacks, Telegram-канал, 2 мая 2022 года, https://t.me/ddos_separ/1186 или https://archive.ph/mecvB.

[48] IT-армия Украины, Telegram-канал, 2 мая 2022 года, https://t.me/itarmyofukraine2022/321 или https://archive.ph/IR1Gv.

[49] Анна Киселева и Маргарита Соболь, «У производителей и дистрибуторов алкоголя возникли сложности с поставками продукции», *Ведомости*, 4 мая 2022 года, https://web.archive.org/web/20220608113248/https://www.vedomosti.ru/business/articles/2022/05/04/920913-u-proizvoditelei-i-distributorov-alkogolya-voznikli-slozhnosti-s-postavkami-produktsii.

[50] IT-армия Украины, Telegram-канал, 7 мая 2022 года, https://t.me/itarmyofukraine2022/331 или https://archive.ph/QkT15.

[51] IT-армия Украины, Telegram-канал, 8 мая 2022 года, https://t.me/itarmyofukraine2022/333 или https://archive.ph/BgFxi.

[52] Министерство иностранных дел Российской Федерации, «Ответ Специального представителя Президента Российской Федерации по международному сотрудничеству в области информационной безопасности, директора Департамента международной информационной безопасности Министерства иностранных дел России А.В. Крутских на вопрос СМИ об атаках на российскую критическую инфраструктуру», 9 июня 2022 г., https://www.mid.ru/ru/foreign_policy/news/1817019/ или https://archive.ph/8U6CN.

[53] Координационный документ IT-армии, дата обращения – 30 марта 2022 года, https://docs.google.com/spreadsheets/d/1xDbYcqCteABOZo3gGGP2uHG-0i3f-UuMGbNZ-Bo_W8Q/edit?usp=drivesdk.

для новичков.[54] Что касается приоритизации целей DDoS-атак, то, согласно документу, в то время у IT-армии было только два типа приоритета. Российские онлайн-банковские сервисы, такие как Сбербанк, и платежные системы, такие как Mirconnect, были признаны целями с приоритетом первого уровня. Работающие онлайн розничные сети и доставка, например, cse[.]ru, расценивались как цели с приоритетом второго уровня. Примечательно, что на момент написания этой статьи сервис QIWI все еще отсутствовал в списке приоритетов, однако он фигурировал на отдельной вкладке под названием «find_ip_port», при этом IP и порты там пока не указаны, что подтверждает ситуативный характер атаки IT-армии на QIWI. Интересно, что в документе также была вкладка под названием «IP и порт», которая на 30 марта включала только URL-адреса, IP-адреса и порты шести российских министерств. Эти цели были опубликованы каналом IT-армии 30 марта в 13:48 по центральноевропейскому времени. Кроме этих шести целей, во всем координационном документе больше не перечислено других IP-адресов и портов.

В целом, IT-армия, в основном, использовала координационный документ в качестве вводного руководства для новичков, поэтому в него было включено две категории уровней DDoS-атак: «атака: простой уровень» и «атака: продвинутый уровень».

Для простого уровня перечислено четыре сайта DDoS-атак. Пользователи загружают эти веб-сайты в свой браузер, затем скрипт с веб-сайта непрерывно отправляет запросы в заранее определенный список назначенных целей атаки. Одни DDoS-сайты отображают информацию об атакуемых сайтах, другие – нет. Вероятно, самым популярным веб-сайтом для проведения DDoS-атак, рекомендованным в соответствии со списком координационного документа IT-армии, является playforukraine[.]org. Данный веб-сайт был разработан членами Львовского IT-кластера и геймифицирует DDoS-атаки, вовлекая пользователей при помощи популярной пазл-головоломки 2048.[55] Playforukraine стоит особняком от других сайтов для проведения DDoS-атак по четырем причинам: (а) он был запущен 28 февраля, всего через четыре дня после начала российского вторжения; (б) утверждается, что он был верифицирован украинской киберполицией; (в) его продвигали на официальном сайте Львовской областной администрации; и (г) он был официально одобрен украинским Министерством цифровой трансформации и даже украинским парламентом.[56]

В интервью *FastCompany* разработчики пояснили, что «один пользователь может отправить 20 000 запросов на сервер за один час игрового процесса».[57] 3 марта Playforukraine написала в Twitter, что «123 тыс. игроков совершили 153 миллиарда атак».[58] Playforukraine не раскрывает, на какие сайты совершается атака, но случайный скриншот, размещенный в их аккаунте в Twitter, показывает результаты веб-проверки dominopizza[.]ru, alfabank[.]ru и gazprom[.]ru.[59] Как и в случае со всеми другими векторами атак, Playforukraine отмечает на своем веб-сайте: «Перед началом игры включите [Виртуальную частную сеть – VPN], если вы играете с территории Украины».[60] По сути это означает, что пользователи, использующие VPN, направляют свой трафик через сервер, расположенный за пределами Украины – преимущественно в странах–членах ЕС и НАТО – для DDoS-атак на российские сайты. Причин для этого множество, и главная из них заключается в том, что российские компании внесли в черный список украинские IP-адреса.

Если говорить о DDoS-атаках продвинутого уровня, то координационный документ IT-армии довольно сильно устарел, поскольку включает в себя пошаговые инструкции, составленные еще в конце февраля. Это такие инструкции, как использование бесплатных пробных периодов для виртуальных серверов в облаке, предлагаемых AWS, Google и Microsoft, для установки средств DDoS–атаки. Другие инструкции охватывают несколько репозиториев GitHub для настройки докеров и «стресс-тестеров/ инструментов тестирования DDoS», включая GoldenEye и Slowloris, которые представляют собой вполне себе традиционные решения.[61] Первые релизы GoldenEye были выпущены еще в 2012 году, а Slowloris – за три года до этого.[62]

Сайт под названием ddosukraine[.]com.ua представляет более четкое понимание того, что IT-армия подразумевает под атаками продвинутого уровня. Изначально было неизвестно, кто создал сайт, но в марте официальный бот канала IT-армии начал каждые 15 минут рекомендовать сайт в Telegram-чате IT-армии. Этот веб-сайт также связан исключительно с каналом IT-армии и обновляется каждые 15 минут для показа самой свежей информации о целях атак, публикуемой IT-армией.[63]

---

[54] После создания официального веб-сайта IT-армии Украины (itarmy.com.ua), ведение координационного документа прекратилось.

[55] Марк Салливан, «В этой игре возможности краудсорсинга применяются для кибератак на российские веб-сайты», *FastCompany*, 18 марта 2022 года, https://web.archive.org/web/20220608145943/https://www.fastcompany.com/90732766/ddos-play-for-ukraine-russian-cyberattack.

[56] PlayforUkraine, Twitter, 28 февраля 2022 года, https://web.archive.org/web/20220509133130/https://twitter.com/playforukraine1/status/1498273795366293505; Loda.gov.ua, «Львівські IT-спеціалісти створили онлайн гру для допомоги Україні у боротьбі з російською агресією», 28 февраля 2022 год, https://web.archive.org/web/20220509121148/https://loda.gov.ua/news?id=65972; Министерство цифровой трансформации, Telegram-канал, 15 марта 2022 года, https://t.me/mintsyfra/2763 или https://archive.ph/LHhEe; Министерство цифровой трансформации, Telegram-канал, 12 апреля 2022 года, https://t.me/mintsyfra/2908 или https://archive.ph/M5LJE; Верховная рада Украины Telegram-канал, 15 марта 2022 года, https://t.me/verkhovnara- daofukraine/1347.

[57] Салливан, «В этой игре возможности краудсорсинга применяются для кибератак на российские веб-сайты».

[58] PlayforUkraine, Twitter, 3 марта 2022 года, https://web.archive.org/web/20220509133153/https://twitter.com/playforukraine1/status/1499425742962184192.

[59] PlayforUkraine, Twitter, 18 марта 2022 года, https://web.archive.org/web/20220509132632/https://twitter.com/playforukraine1/status/1504797556513067013; PlayforUkraine, Twitter, 17 марта 2022 года, https://web.archive.org/web/20220509132848/https://twitter.com/playforukraine1/status/1504487841467826189; PlayforUkraine, Twitter, 5 марта 2022 года, https://web.archive.org/web/20220509132906/https://twitter.com/playforukraine1/status/1500161959911731201.

[60] PlayforUkraine, веб-сайт, 9 мая 2022 года, https://web.archive.org/web/20220509133002/https://playforukraine.org/.

[61] GoldenEye, веб-сервис Github, дата обращения – 8 июня, https://web.archive.org/web/20220608104809/https://github.com/jseidl/GoldenEye; Slowloris, веб-сервис Github, дата обращения – 8 июня, https://web.archive.org/web/20220608095923/https://github.com/gkbrk/slowloris.

[62] репозиторий Zion3r, «[GoldenEye v2.0] DoS Tool», Kitploit.com, 23 января 2014 года, https://web.archive.org/web/20220613151215/https://www.kitploit.com/2014/01/goldeneye-v20-dos-tool.html?m=0; RSnake и Джон Кинселла, «Slowloris HTTP DoS», ha.ckers.org, дата обращения – 8 июня, https://web.archive.org/web/20090822001255/http://ha.ckers.org/slowloris/.

[63] DDoSUkraine, веб-сайт, 1 апреля 2022 года, https://web.archive.org/web/20220401160219/https://ddosukraine.com.ua/.

В разделе «powerful tools» («мощные инструменты») в одном из наборов инструкций подробно описывается, как настроить виртуальную машину для запуска инструмента DDoS-атак «Death by 1000 needles» (db1000n). Db1000n – это репозиторий GitHub, автором которого является Arriven aka. Богдан Ивашко, старший инженер-программист, работающий в Киеве, в компании Cyberhaven со штаб-квартирой в Пало-Альто, США, занимающейся безопасностью компьютерных сетей.[64] Специфика инструмента Db1000n состоит в том, что (а) он был загружен на GitHub 26 февраля, как прямой ответ на российское вторжение, (б) в его официальном руководстве отмечается, что «это руководство по использованию для тех, кто хочет предоставить свои компьютеры для целей централизованного управления Украинской IT-армией», (в) он упоминается более 680 раз в чате IT-армии и (г) он служит основой для нескольких копий git clone, созданных вследствие функционирования IT-армии.[65]

Например, инструкции для db1000n на сайте ddosukraine[.]com связаны с папкой Google Drive с файлом формата docx, в котором написано следующее: «Меня зовут Игорь, я IT-специалист из Львова. Сначала я наткнулся на канал «IT-армия Украины» в Telegram. Там я узнал, что существует готовая программа «Death by 1000 needles», созданная для обрушивания сайтов Мордора, а также что ее нужно запускать через VPN. За неделю я собрал виртуальную оболочку для Death by 1000 needles. Она оказалась довольно удачной, поэтому я решил поделиться ей с другими пользователями».[66]

В начале апреля сайт ddosukraine[.]com.ua перенесен на новый домен itarmy[.]com.ua. С тех пор этот сайт продвигается официальным ботом IT-армии, а канал IT-армии одобрил его как официальный веб-сайт IT-армии Украины. Вероятно, самым интригующим изменением, объявленным на новом сайте, стало объявление от 5 апреля, в котором говорилось: «Очень важно! Для эффективной атаки мы все должны наносить удары по одним и тем же целям и так долго, как это необходимо. Поэтому мы просим вас не вступать в чаты и не предпринимать самостоятельных атак на другие цели».[67]

Репозитории GitHub

На момент написания данной статьи самый обсуждаемый в чате IT-армии репозиторий GitHub, с примерно 1070 упоминаниями, называется MHDDoS. MHDDoS никоим образом не аффилирован с IT-армией, и его автор прямо отмечает в файле «readme» репозитория: «Пожалуйста, не атакуйте веб-сайты без согласия владельца».[68] Наиболее распространенный клон MHDDoS в чате IT-армии называется MHDDoS_proxy, и его автором является пользователь с именем porthole-ascend-cinnamon.[69] В файле readme репозитория GitHub porthole-ascend-cinnamon ссылается на неофициальное руководство под названием «DDoS-for-all» («DDoS-атаки для всех»), автором которого является пользователь по имени SlavaUkraineSince1991.[70] Неудивительно, что примерами, которые SlavaUkraineSince1991 использовал в своем руководстве, были ria[.]ru и tass[.]ru. Что стало неожиданностью, так это то, что руководство ссылалось на три разных канала Telegram, и ни один из них не был каналом IT-армии непосредственно: «DDOS Tutorial for all» («Учебник по DDOS-атакам для всех») (около 5800 подписчиков), «KiberBull» (около 7700 подписчиков) и «Украинский жнец (Ukrainian Reaper) (около 4800 подписчиков).[71]

При взгляде на три канала, о которых идет речь, бросается в глаза несколько вещей. Все три канала время от времени выбирают цели, о которых сообщает канал IT-армии. Например, KiberBull был единственным каналом (из доступных мне для просмотра), который 14 марта перепостил информацию о том, что целью атаки выбрана asna[.]ru. Для сравнения, 1 марта канал «Украинский жнец» официально заявил, что для них источником информации о целях атаки является канал IT-армии и Telegram-канал под названием «ddoskotyky» (около 20 100 подписчиков).[72] В некоторых случаях «Учебник по DDOS-атакам для всех» и Kiberbull принимали решение помочь IT-армии покончить с их целями, как это было 19 марта, когда IT-армия объявила о нападении на Tutu[.]ru – крупнейший в России сервис бронирования железнодорожных и авиабилетов. «Учебник по DDOS-атакам для всех» пояснил, что «мы помогаем IT-армии Украины прикончить tutu[.]ru», а KiberBull также написал, что «мы поможем IT-Армии вывести из строя одну из крупнейших служб бронирования билетов [tuttu[.]ru]».[73] В целом, однако, эти три канала, вероятно, не действуют как

[64] Db1000n, ReadMe.md, веб-сервис Github, 8 июня 2022 года, https://web.archive.org/web/20220608094714/https://github.com/Arriven/db1000n; Arriven, веб-сервис Github, 8 июня 2022 года, https://web.archive.org/web/20220608094644/https://github.com/arriven; Cyberhaven, «Наша миссия», дата обращения – 8 июня, https://www.cyberhaven.com/about-us/.

[65] Db1000n, Релизы, веб-сервис Github, 8 июня 2022 года, https://web.archive.org/web/20220608094937/https://github.com/Arriven/db1000n/releases?page=9; Death by 1000 needles, 24 марта 2022 года, https://web.archive.org/web/20220324210843/https://telegra.ph/death-by-1000-needles-03-18; Db1000n Hotspotshield, веб-сервис Github, 8 июня 2022 года, https://web.archive.org/web/20220608095015/https://github.com/gidiyan/db1000n_hotspotshield.

[66] Google-перевод: https://docs.google.com/document/d/1puI2_V5_oyc1cA4a3yuwl8J2_O4ooybOHuU1fR261k/edit. Название документа неизвестно, ссылка актуальна по состоянию на март 2022 года.

[67] IT-армия Украины, 5 апреля 2022 г., https://web.archive.org/web/20220405192723/https://itarmy.com.ua/.

[68] MatrixTM, MHDDoS, Readme.md, веб-сервис Github, 8 июня 2022 года, https://web.archive.org/web/20220608095847/https://github.com/MatrixTM/MHDDoS/blob/main/README.md.

[69] Porthole-ascend-cinnamon, MHDDoS_proxy, Readme.md, Github, 8 июня 2022 года, https://web.archive.org/web/20220608105000/https://github.com/port- hole-ascend-cinnamon/mhddos_proxy.

[70] SlavaUkraineSince1991, DDoS-for-all, MHDDoS_proxy.md, Github, 8 июня 2022 года, https://web.archive.org/web/20220608104915/https://github.com/SlavaUkraineSince1991 1/DDoS-for-all/blob/main/MHDDoS_proxy.md.

[71] Примечание: «Украинский жнец», вероятно, был включен в список, потому что их инструмент множественных DDoS-атак частично построен на MHDDoS_proxy. См. Украинский жнец, «Український жнець на зв'язку. DDOS-имо РФ за допомогою Multiddos», *Mezha (Межа)*, 21 мая 2022 года, https://web.archive.org/web/20220608104948/https://mezha.media/articles/ddos-rf-z- multiddos/.

[72] Украинский жнец, Telegram-канал, 1 марта 2022 года,https://t.me/ukrainian_reaper_ddos/5 или https://archive.ph/5W3Jo.

[73] DDoS Tutorial for All, Telegram-канал, 19 марта 2022 года, https://t.me/ddos_for_all/103 или https://archive.ph/Io3lq.

одна согласованная группа, за исключением одной странности: «Учебник по DDOS-атакам для всех» действительно время от времени поддерживает KiberBull и «Украинского жнеца» в компаниях, проводимых последними самостоятельно, т.е. независимо от назначения целей DDoS-атак со стороны IT-армии.[74]

Следует ли считать, что эти три группы все-таки входят в состав IT-армии? И да, и нет. С одной стороны, они иногда участвуют в DDoS-кампаниях IT-армии. С другой стороны, сама IT-армия пояснила в сообщении Telegram от 4 апреля: «Существует довольно много каналов, которые проводят DDoS-атаки на враждебные сервисы вместе с нами. Каждое сообщество имеет свою базу данных учебных пособий, а также достаточное количество вовлеченных участников. Важно понимать, что каждое сообщество независимо и само выбирает для себя приоритетные цели. Но мы все общаемся друг с другом, и довольно часто они поддерживают нас в атаках на наши цели. Мы хотим поблагодарить наших подписчиков и следующие сообщества за их активную позицию и помощь в борьбе с врагом в киберпространстве».[75] Среди перечисленных сообществ: «Украинский жнец» и KiberBull, а также Cyber Palyanitsa, Studentcybergroup, DDoS Attack Cyber Cossacks, Anonymous-Ukraine, DDoS Joint Group и UA Cyber Shield, которые мы рассмотрим далее.

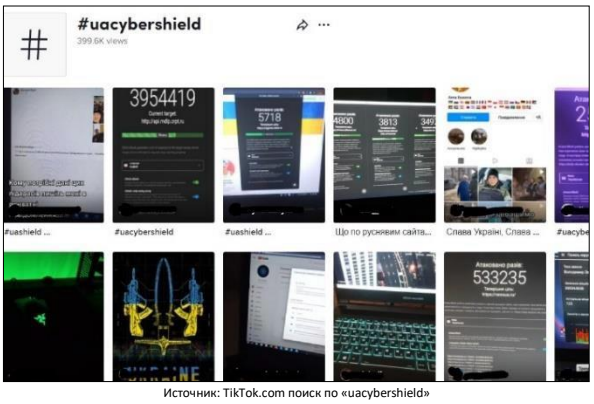
Заметка на полях: Подход Cyber Palyanitsa по своей манере напоминает подход IT-армии: На веб-сайте данного ресурса перечисляется несколько координационных групп и приводится рекомендация: «Выбери свой легион. У каждой из наших групп есть как общие, так и индивидуальные задачи, присоединяйтесь и помогайте Украине вместе с нами!»[76]

Источник: cyberarmy[.]com.ua

Третий репозиторий GitHub, который всплывает в различных каналах Telegram, называется UA Cyber Shield, или сокращенно: uashield. Unishield – это инструмент DDoS-атак, который был загружен на GitHub 28 февраля. Это проект группы, которая называет себя «Добровольческая кибероборона Украины». Uashield примечателен за счет четырех имеющихся странностей:
(а) на веб-сайте группы – help-ukraine-win.super[.]site – отображается официальный логотип украинского правительства с пометкой «поддерживается Кабинетом Министров Украины»; (б) в файле readme репозитория GitHub содержится пояснение «ВНИМАНИЕ!!! Мы не поддерживаем незаконные активные атаки, или вредоносные кампании, которые наносят технический ущерб. Использовать только в образовательных целях. Вы можете попробовать применить эту платформу только на своем собственном сайте!», (в) это единственный известный мне инструмент DDoS-атак, инструкции которого переведены на 11 различных языков, включая корейский и португальский; и (г) 31 марта официальный Telegram-канал uashield заявил, что «начиная с текущей версии UA Cyber SHIELD поддерживает все типы атак, используемые IT-армией Украины: HTTP / HTTPS / UDP».[77] Четыре дня спустя uashield официально объявила, что «мы работаем вместе с IT-АРМИЕЙ Украины».[78]

Источник: help-ukraine-win.super[.]site

Примечательно, что uashield, работающий практически со всеми операционными системами, включая мобильные ОС, а также имеющий прекрасный интерфейс для атаки контр-пользователя, совершенно естественно привлек внимание многих молодых пользователей, не являющихся техническими специалистами, которые, в свою очередь, опубликовали несколько видеороликов в TikTok о своем опыте использования uashield.[79]



Источник: TikTok.com поиск по «uacybershield»

[74] DDoS Tutorial for All, Telegram-канал, 21 March 2022 года, https://t.me/ddos_for_all/110 или https://archive.ph/xFH98; DDoS Tutorial for All, Telegram-канал, 19 марта 2022 года, https://t.me/ddos_for_all/102 или https://archive.ph/bamMR.

[75] IT-армия Украины, Telegram-канал 4 апреля 2022 года, https://t.me/itarmyofukraine2022/265 или https://archive.ph/ANHcd.

[76] Cyber Palyanitsa, веб-сайт, дата обращения – 17 июня 2022 года, https://web.archive.org/web/20220617064032/https://cyberarmy.com.ua/

[77] UA Cyber Shield, «Помоги Украине победить» дата не указана, https://web.archive.org/web/20220509131644/https://help-ukraine-win.super.site/; Opengs, uashield, readme-en.md, Github, 8 июня 2022 года, https://web.archive.org/web/20220608105100/https://github.com/opengs/uashield/blob/master/README-en.md; UA Cyber Shield, «KR - Help Ukraine», дата обращения – 9 мая, https://web.archive.org/web/20220509131841/https://help-ukraine-win.super.site/kr-help-ukraine; UA Cyber Shield, Telegram-канал, 31 марта 2022 года, https://t.me/uashield/22 или https://archive.ph/QKlqY.

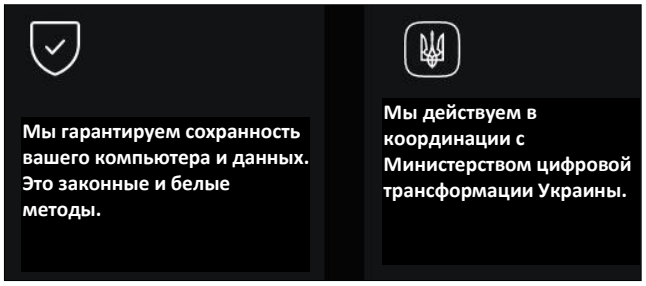
[78] UA Cyber Shield, Telegram-канал, 4 апреля 2022 года, https://t.me/uashield/33 или https://archive.ph/dfGOf.

[79] Поиск в Tiktok по «uashield» и «uacybershield», https://www.tik- tok.com/tag/uashield; https://www.tiktok.com/tag/uacybershield.

Четвертый репозиторий GitHub называется disBalancer. DisBalancer был разработан командой энтузиастов в сфере кибербезопасности и криптовалют и запущен под собирательным названием Hacken Foundation 2 марта 2021 года. Он позиционирует себя как децентрализованная сеть защиты от DDoS-атак web3. По сути, пользователи по всему миру могут установить disBalancer и стать пользователями (или «фермерами», как их здесь называют) децентрализованной сети, сдав в аренду неиспользуемые ресурсы (пропускную способность) и место для хранения. Взамен они получают DDoS-токены, которые можно покупать и продавать на большинстве бирж криптовалют. Как поясняет disBalancer: «Это работает аналогично майнинг-пулу блокчейна, за счет настройки компьютерного узла для выполнения необходимых операций и получения трафика».[80] Компании, заинтересованные во внедрении disBalancer в качестве решения для защиты от DDoS-атак, просто должны добавить свои сетевые узлы в записи DNS, и «весь трафик начнет циркулировать за ближайшими доступными узлами. Затем каждый узел может перенаправлять трафик на соседние узлы, чтобы увеличить пропускную способность по мере необходимости».[81] По своей сути disBalancer задумывался как защитный инструмент для разгрузки входящего DDoS-трафика. Как поясняет сама команда, «мы стремимся защитить компании с серверами и сервисами в Интернете от DDoS-атак. Наша сеть будет действовать как гарант, делясь неиспользуемой компьютерной мощностью и пропускной способностью с компаниями, которым нужны эти ресурсы. Так мы сделаем мир более безопасным и изменим значение DDoS в лучшую сторону».[82] И на том спасибо.

4 Hacken, Liberator и Hackenproof

Проблема для Hacken.io со штаб-квартирой в Эстонии началась 4 марта, когда команда disBalancer запустила инструмент DDoS-атаки под названием Liberator. Liberator был разработан в ответ на российское вторжение с главной целью «помощи в освобождении Украины» путем проведения DDoS-атак на «российские пропагандистские веб-сайты и источники, которые способствуют российскому вторжению на Украину».[83] Команда disBalancer фактически переключилась с защиты от DDoS-атак на DDoS-атаки, объяснив: «Не спрашивайте нас, насколько легальны DDoS-атаки на российские пропагандистские сайты. Наши города подвергаются бомбардировкам, в которых гибнут дети и мирные жители. Мы действуем по согласованию с Министерством цифровой трансформации, которое инициировало создание «Украинской киберармии» [IT-армии] для помощи Вооруженным силам Украины».[84] Подключившись к сообществу, которое disBalancer создал за последний год, пользователи по всему миру, которые ранее использовали инструмент disBalancer для защиты от DDoS-атак, теперь прислушались к призыву и установили Liberator для использования его в наступательных целях. Более того, disBalancer также напомнил своим подписчикам, что «если вы считаете, что это вас не касается или не согласны с нашим участием в борьбе с российской агрессией, просто покиньте нас навсегда. Равнодушие – не меньшее преступление, когда дело касается чужих жизней».[85] На момент написания этой статьи disBalancer утверждал, что Liberator был загружен более 100 000 раз, и что в любой заданный момент времени от 3000 до 6000 пользователей запускают данное приложение. На случай, что этого недостаточно, чтобы убедить людей принять участие, на сайте disBalancer отмечается, что (а) «мы гарантируем безопасность вашего компьютера и данных. Это легальные и белые методы» и что (б) «покупая DDoS-токены, любой может помочь нам масштабировать инфраструктуру приложений и приобрести больше серверов».[86] Это означает, что DDoS-токены, которые пользователи могли получить, будучи частью децентрализованной сети защиты от DDoS-атак disBalancer, теперь используются в качестве финансового ресурса для создания инфраструктуры DDoS-атак Liberator. Если после этого пользователи все еще сомневаются, стоит ли устанавливать Liberator, сайт disBalancer заверяет их, разместив сверху украинский герб, что «мы действуем по согласованию с Министерством цифровой трансформации Украины».[87]



Источник: disbalancer.com

Итак, насколько тесно disBalancer взаимосвязан с Hacken и Министерством цифровой трансформации? Для примера, лидеры команды disBalancer показаны на их веб-сайте на видном месте. Среди них Сергей Долгополый, который работает техническим руководителем, а также входит в киевскую команду Hacken по исследованиям и разработкам.[88]

[80] disBalancer, «Представляем disBalancer: Децентрализованная защита от DDoS-атак», веб-ресурс Medium, 2 марта 2021 года, https://web.archive.org/web/20220509130352/https://disbalancer.medium.com/introducing-disbalancer-decentralized-ddos-protection-b5fdb8fcf37f.

[81] Там же.

[82] disBalancer, «Кто мы» веб-сайт disbalancer.com, дата не указана https://web.archive.org/web/20220509125532/https://disbalancer.com/about/.

[83] disBalancer, «disBalancer запускает Liberator», веб-ресурс *Medium*, 4 марта 2022 года, https://web.archive.org/web/20220509125831/https://disbalancer.medium.com/disbalancer-launches-liberator-a6c145cb88e4.

[84] disBalancer, «disBalancer на стороне Украины», веб-ресурс *Medium*, 1 марта 2022 года, https://web.archive.org/web/20220509130008/https://disbalancer.medium.com/disbalancer-stays-with-ukraine-689327e0edf6.

[85] Там же.

[86] disBalancer, веб-сайт, дата обращения – 10 мая, https://web.archive.org/web/20220510123739/https://disbalancer.com/.

[87] Там же.

[88] Сергей Довгополый, Linkedin, дата обращения – 8 июня, https://www.linkedin.com/in/sdovhopolyi/?originalSubdomain=ua.

Александр Горлан руководит операционной деятельностью, а также работает в Hacken в Киеве в качестве тестировщика на проникновение и аналитика по безопасности.[89] Дима Будорин является советником, а также соучредителем и генеральным директором Hacken.[90] Наконец, Денис Иванов является советником, а также руководителем экспертной группы в Министерстве цифровой трансформации.[91] В уведомлении о конфиденциальности веб-сайта disBalancer аналогичным образом объясняется, что «мы – компания Hacken OÜ, расположенная по адресу Kai tn 1-5M, город Таллинн, Харьюмаа, 10111, Эстония».[92] Это физический адрес штаб-квартиры Hacken в Эстонии – стране-члене НАТО и ЕС.

Интересно, что 10 марта *Politico* сообщила, что около 50 сотрудников киевского офиса Hacken были переведены в Испанию – еще одно государство-член НАТО/ЕС – по соображениям безопасности.[93] Восемнадцать дней спустя канал IT-армии впервые официально прорекламировал Liberator от disBalancer среди своих на тот момент 306 000 подписчиков.[94]

20 апреля disBalancer опубликовала свое первое мобилизационное видео на Youtube. В сообщении к видео говорилось: «Инструкция понятна даже маленькому ребенку. Самое эффективное DDoS-приложение против российского агрессора. […] Проводите атаки 24/7, где бы вы ни находились. Мы – Киберармия. Присоединяйтесь к Украинской Киберармии в первой мировой кибервойне. Вы можете стать легендой».[95] Восемь дней спустя криптоинфлюэнсер по имени Boxmining опубликовал на своем Youtube-канале 8-минутное видео, в котором призвал 268 000 своих подписчиков установить Liberator для проведения DDoS-атак на сайты в России.[96] Boxmining – это не просто случайный инфлюэнсер с Youtube. Он посещал киевский офис Hacken в 2020 году, а в 2021 году взял интервью у генерального директора Hacken Димы Буродина на своем канале Youtube. Естественно, видео с энтузиазмом подхватили disBalancer и Telegram-канал Hacken Forces, а также аккаунт Hacken в Twitter, который разместил твит «как защитить Украину с помощью ОДНОГО приложения? Запустите Liberator от disBalancer! @boxmining, известный криптоинфлюэнсер и друг Hacken, выпустил новое видео на своем канале Youtube с простыми иснтрукциями».[97]

Ни Hacken, ни Boxmining не проинформировали своих (в основном молодых) пользователей о потенциальных юридических последствиях запуска DDoS-атак и вмешательства в международный вооруженный конфликт. В США DDoS-атаки могут считаться федеральным преступлением в соответствии с Законом о борьбе с компьютерным мошенничеством и компьютерными злоупотреблениями.[98] А в Эстонии, где физически находится штаб-квартира Hacken, DDoS-атаки могут подпадать под категорию компьютерного саботажа, наказуемого лишением свободы на срок до 3 лет.[99] Примечательно, что еще в начале апреля 2022 года ФСБ России задержала системного администратора, работавшего в местной компании в Ялте, Крым, который установил на свой рабочий компьютер DDoS-инструмент для проведения атак на российские сайты в период с 24 февраля по 10 марта.[100] В настоящее время ему грозит пять лет лишения свободы. Неизвестно, какой именно инструмент DDoS-атаки он использовал. Что нам известно точно, так это то, что в середине мая The Wall Street Journal сообщил, что киевская команда disBalancer/Hacken переехала из Барселоны (Испания) в Лиссабон (Португалия), т.е. еще одно государство-член НАТО и ЕС.[101]

Словно в подтверждение такой беззаботности, disBalancer решил опубликовать три интервью с пользователями Liberator от 27 мая 2022 г.[102] Неизвестно, были ли эти интервью проведены с реальными пользователями или придуманы командой disBalancer для рекламы использования Liberator. Джейс Мо из США заявил: «Я начал со страницы hackenproof.com и просто пошел дальше. Оказалось, что Liberator «ЧЕРТОВСКИ ПРОСТ» (англ. Easy AF) в использовании. […]. Liberator не только «чертовски» упростил участие в борьбе, но и позволил обычному человеку стать частью команды,проводящей самую масштабную и эффективную DDoS-атаку, которую когда-либо видел мир. Люблю это дерьмо».[103] Тем временем Казимир из Германии подчеркнул финансовую сторону дела:

---

[89] Александр Горлан, Linkedin, дата обращения – 8 июня, https://www.linkedin.com/in/sdovhopolyi/?originalSubdomain=ua.

[90] Диа Будорин, Linkedin, дата обращения – 8 июня, https://www.linkedin.com/in/dyma-budorin-acca-56a98035/?originalSub- domain=ua.

[91] Денис Иванов, Linkedin, дата обращения – 8 июня, https://www.linkedin.com/in/daivanov/?originalSubdomain=ua.

[92] disBalancer, «Уведомление о конфиденциальности “DisBalancer”», disBalancer, 16 февраля 2022 года, https://disbalancer.com/legal/PrivacyNotice.pdf.

[93] Лоуренс Церулус, «Киевские хакеры воспользовались моментом военного времени», *Politico*, 10 марта 2022 года, https://www.politico.eu/article/kyiv-cyber-firm-state-backed- hacking-group/ или https://archive.ph/qdyD5.

[94] IT-армия Украины, Telegram-канал, 28 марта 2022 года, https://t.me/itarmyofukraine2022/245 или https://archive.ph/JobpV

[95] disBalancer, «Присоединятесь к disBalancer, чтобы бороться с русской пропагандой», Youtube, 19 апреля 2022 года, https://www.youtube.com/watch?v=iCPwat9G6kA.

[96] Boxmining, «МНЕ НУЖНА ВАША ПОМОЩЬ! Как ВЫ можете поддержать Украину с помощью ОДНОГО приложения (DISBALANCER)», Youtube, 28 апреля 2022 года, https://youtu.be/k9LwqbowGMk.

[97] disBalancer, Telegram-канал, 28 апреля 2022 года, https://t.me/disbalancer_offi- cial/427 или https://archive.ph/94aPY; Hacker Forces, Telegram-канал, 28 апреля 2022 года, https://t.me/hackencyberarmy/240 или https://archive.ph/nVu3l; Hacken, Twitter, 28 апреля 2022 года, https://web.archive.org/web/20220509135045/https://twitter.com/hackenclub/status/1519728201941012481.

[98] Исследовательская служба Конгресса, «Киберпреступность и закон: Закон о компьютерном мошенничестве и злоупотреблениях (CFAA) и 116-й Конгресс», 21 сентября 2020 года, https://sgp.fas.org/crs/misc/R46536.pdf, стр. 14; Практическое право Томаса Рейтера, «Распределенная атака типа “Отказ в обслуживании” (DDoS)», дата обращения – 8 июня, https://web.archive.org/web/20220615115331/https://ca.practical-law.thomsonreuters.com/7-516-9293?transitionType=Default&context-Data=(sc.Default)&firstPage=true.

Шон Тума: «Да, прецедентное право гласит, что DDoS-атака на веб-сайт действительно является нарушением CFAA», shawnetuma.com, 9 октября 2013 года, https://web.archive.org/web/20220615113618/https://shawnetuma.com/2013/10/09/yes
-case-law-says-it-really-is-a-cfaa-violation-to-ddos-a-website/.

[99] Riigi Teataja, «Уголовный кодекс Эстонии: §207(1) – Воспрепятствование функционированию компьютерных систем», riigiteataja.ee, 1 января 2015 г., https://www.riigiteataja.ee/en/eli/522012015002/consolide.

[100] Positive Technologies, «ФСБ задержала жителя Ялты за кибератаки на российские информационные ресурсы», SecurityLab, 9 April 2022, https://www.securitylab.ru/news/531066.php или https://archive.ph/paTDo.

[101] Дэвид Уберти: «Они бежали из Украины, чтобы сохранить жизнь своему киберстартапу. Теперь они наносят ответный кибердар», The Wall Street Journal, 12 мая 2022 г., https://www.wsj.com/articles/they-fled-ukraine-to-keep-their-cyber-startup-alive-now-theyre-hacking-back-11652347802.

[102] disBalancer, «disBalancers поделился своими историями кибербоев», *disBalancer*, 27 мая 2022 г., https://web.archive.org/web/20220529121248/https://blog.disbalancer.com/disbalancers-shared-their-cyber-fight-stories /.

[103] Там же.

«Что могло бы мотивировать меня еще больше? Возможно, особый вид disBalancer-NFT для проверенных пользователей Liberator. ;) Я видел, что существуют DDOS-NFT для тех, у кого есть более 1000 DDOS [токенов], пока война не закончится (что для меня просто, потому что я покупаю так много, как только могу)… Но, может быть, вы могли бы сделать специальное издание NFT для кибервоинов?»[104] А Даниил из Украины выделил то, что еще можно сделать: «Помимо участия в disBalancer, я активно поддерживаю Украину и другими способами. Например, делая пожертвования вооруженным силам Украины и помогая кибервойне на стороне украинцев с помощью других инструментов DDoS, предназначенных для подрыв деятельности россиян. Я использую несколько других приложений, таких как UA Cyber SHIELD, dn1000n, dripper, MHDDos и 5 сайтов для DDoS-атак. Кроме того, я сообщаю [администрации Telegram] о российских пропагандистских группах в Telegram, чтобы помешать лжи, распространяемой среди людей, в том числе на оккупированных территориях».[105]

8 июня 2022 года disBalancer объявил, что Роскомнадзор – Федеральная служба России по надзору в сфере связи, информационных технологий и массовых коммуникаций – заблокировал доступ к disbalancer[.]com.[106] Согласно блогу disBalancer, «ограничения доступа к нашему сайту для российских провайдеров и интернет-пользователей из России не остановят наши DDoS-атаки на российские пропагандистские сайты, правительственные и инфраструктурные системы, которые составляют основу повседневной жизни и обеспечивают поток товаров, информации и услуг. До тех пор, пока Россия не выведет из Украины последнего солдата и продолжающиеся обстрелы со стороны российских войск не прекратятся, мы намерены и дальше наращивать нашу активность».[107]

Сотрудничество между Hacken и украинским правительством на этом не заканчивается. HackenProof, являющаяся платформой bug bounty (с помощью, которой люди могут получить признание и вознаграждение за нахождение ошибок, особенно тех, которые касаются эксплойтов и уязвимостей) Hacken, запустила две программы сообщений об уязвимостях в ответ на продолжающуюся войну на Украине: защитную и наступательную. Оборонительная программа была создана примерно 1 марта и проходит под названием «Призыв к киберзащите Украины. Остановим войну».[108] Она направлена на поиск «критических уязвимостей» в украинских правительственных и инфраструктурных веб-сайтах, о которых HackernProof затем сообщает соответствующим органам. Как поясняется на сайте, «мы ищем уязвимости, такие как RCE, SQLI, RFI/LFI или утечки данных. Пожалуйста, не тратьте время на уязвимости низкой/средней степени тяжести. Сэкономьте наше время для того, что имеет значение».[109] По состоянию на 25 мая в программу поступила 291 заявка от 27 авторов.[110] По данным Wayback Machine, на 8 марта число заявок составило 271 от 23 авторов[111] Таким образом, за последние 2,5 месяца в программу добавилось всего 20 новых заявок.

Хотя программа не выплачивает никаких вознаграждений, важно понимать, что в течение длительного времени этическим хакерам «могло грозить штраф в размере до 42 000 долларов США или даже три года тюремного заключения за попытку обнаружить ошибки в компьютерных системах украинского парламента, министерств или государственных компаний».[112] Только 21 апреля, примерно через семь недель после того, как HackenProof запустил свою защитную программу bug bounty, украинский парламент принял закон «О внесении изменений в Уголовный кодекс Украины относительно повышения эффективности борьбы с киберпреступностью в условиях действия военного положения», который дает разрешение на программы bug bounty для государственного сектора.[113] На момент написания этой статьи все еще неясно, нарушала ли когда-либо программа bug bounty от HackenProof украинское законодательство и защищает ли ее от судебного преследования нахождение на территории Эстонии. Также неизвестно, была ли программа поддержана членами украинского правительства, и как именно HackenProof оптимизировала свой информационный поток, чтобы связаться с множеством заинтересованных украинских государственных органов и компаний.

Наступательная программа HackenProof была запущена 27 февраля и работает под названием «Призыв к эксплойтам. Остановим войну».[114] Подобно защитной программе, HackenProof ищет только сообщения о критических уязвимостях, включая утечки данных, которые затем «передаются в надежные руки украинских кибервойск».[115] Основными направлениями являются российские хостинг-провайдеры, интернет-провайдеры, аэрокосмическое/ воздушное управление, системы SCADA, банки, государственные службы, энергетика/ нефть/ газ, транспорт/

[104] Там же.

[105] Там же.

[106] disBalancer, «Роскомнадзор заблокировал доступ к сайту disBalancer», disBalancer, 8 июня 2022 года, https://blog.disbalancer.com/roskomnadzor-has-blocked-access-to-disbalancer-website/.

[107] Там же.

[108] HackenProof, «Призыв к киберзащите Украины. Остановим войну», 8 марта 2022 года, https://web.archive.org/web/20220308143814/https://hackenproof.com/ukraine-will-win/call-for-ukrainian-cyber-defense-stop-the-war.

[109] Там же.

[110] HackenProof, «Призыв к киберзащите Украины. Остановим войну», 25 марта 2022 г., https://web.archive.org/web/20220525133418/https://hackenproof.com/ukraine-will-win/call-for-ukrainian-cyber-defense-stop-the-war.

[111] HackenProof, «Призыв к киберзащите Украины. Остановим войну», 8 марта 2022 года, https://web.archive.org/web/20220308143814/https://hackenproof.com/ukraine-will-win/call-for-ukrainian-cyber-defense-stop-the-war.

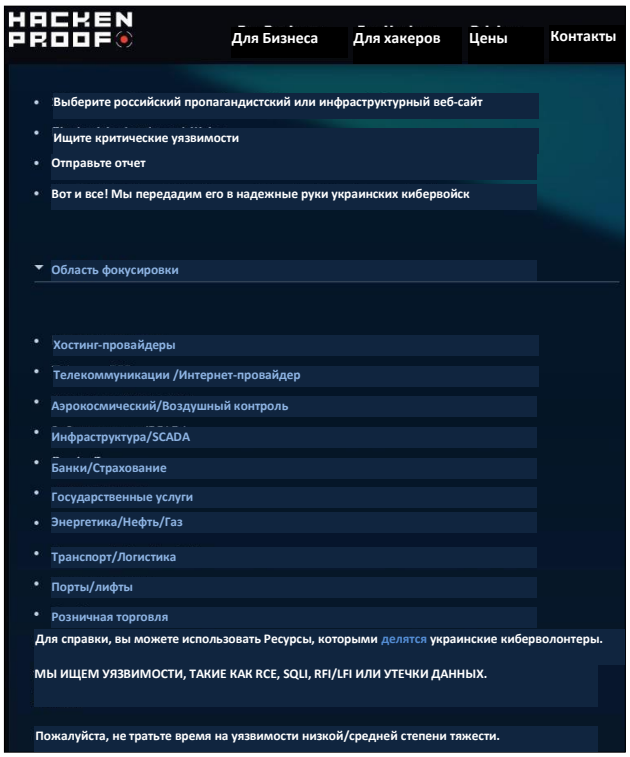
[112] Дарина Антонюк, «Украина пересматривает вознаграждение за нахождение ошибок (bug bounties) после последних кибератак.
Но достаточно ли этого?», *The Record*, 3 февраля 2022 года, https://web.archive.org/web/20220608150708/https://therecord.media/ukraine-reconsiders-bug-bounties-after-latest-cyberattacks-but-are-they-enough/.

[113] Укринформ, «Рада усилила способности национальной системы кибербезопасности», 24 марта 2022 года, https://web.archive.org/web/20220608150618/https://www.ukrinform.ua/rubric-technology/3438840-rada-posilila-spromoznosti-nacionalnoi-sistemi-kiber-bezpeki.html.

[114] HackenProof, «Призыв к эксплойтам. Остановим войну», 27 марта 2020 года, https://web.archive.org/web/20220227105814/https://hackenproof.com/ukraine-will-win/save-millions-lives-hackers-against-russia.

[115] Там же.

логистика, порты/элеваторы и даже розничная торговля. Неясно, принимаются ли HackenProof также заявки, относящиеся к российскому сектору здравоохранения, гуманитарным НПО, школам и университетам. Примечательно, что сайт программы напрямую ссылается на Telegram-канал IT-армии, поясняя: «Для справки, вы можете использовать Ресурсы, которыми делятся украинские киберволонтеры».[116] По состоянию на 25 мая в программе было 422 заявки от 32 авторов.[117] Согласно Wayback Machine, это число остается неизменным с 14 марта.[118] Таким образом, за последние одиннадцать недель наступательная программа не получила новых заявок. Как и в защитной программе, выплаты вознаграждений (bounty pay-outs) также отсутствуют.



Источник: hackenproof.com/ukraine-will-win/save-millions-lives-hackers-against-russia

Удивительно, но существование наступательной программы bug bounty в сочетании с тем фактом, что она организована компанией со штаб-квартирой в Эстонии, до сих пор не вызвало каких-либо юридических, этических или политических дискуссий на тему совместной войны в киберпространстве, роли украинских компаний, действующих из стран-членов НАТО/ЕС, и их атаки на российскую гражданскую инфраструктуру при сотрудничестве с украинским правительством. В сообществе информационной безопасности также совсем не поднимается вопрос роли программ bug bounty, атакующих одну из воюющих сторон международного конфликта. Нынешнее молчание по этим вопросам на фоне продолжающейся войны на Украине, безусловно, понятно, равно как и активизм украинцев за рубежом, и в то же время весьма вероятно, что государства-члены НАТО/ЕС сейчас непреднамеренно создают правовые и этические прецеденты, которые могут иметь значительные политические последствия в будущем. Например, что, если принадлежащая России компания, расположенная в Германии, организует наступательную программу bug bounty, которая будет нацелена на украинскую критическую инфраструктуру и передаст информацию об обнаруженных уязвимостях российской разведке? Сочтут ли Берлин, Брюссель и Вашингтон такое поведение частного сектора приемлемым?

Помимо двух программ bug bounty от HackenProof, Егор Аушев также запустил собственную программу bug bounty под названием «Hack/Fuck Russia», первая фаза которой проходила с 1 по 10 марта. Он был финансово поддержан киевской компанией Cyber Unit Tech, Аушева, пожертвовавшей 100 000 долларов США.[119] Любопытно, что объявление о bug bounty также включало адрес кошелька Tether для пожертвований. На сегодняшний день в этот кошелек было положено в общей сложности 70 Tether, что составляет всего 70 долларов США (Tether привязан к доллару США в соотношении 1:1).[120] Тем не менее, в интервью The Record технический представитель Cyber Unit объяснил, что «наша компания внесла первоначальные 100 000 долларов, но мы видим участие и вклад со всего мира. Суммы очень, очень значительны и могут оказаться в числе самых больших наград за всю историю или, возможно, самой большой “неофициальной” наградой»[121].

Так как же сопоставить эти две разные оценки? Если в основе программы bug bounty Аушева и лежит огромный поток пожертвований, он в любом случае не поступает в кошелек Tether. Нам также известно, что ни Аушев, ни Cyber Unit Tech не размещали никаких других адресов кошельков в своих официальных аккаунтах в Twitter, LinkedIn и Facebook. Итак, как люди со всего мира узнают, в какие кошельки направлять пожертвования в поддержку этого дела? Одним из возможных объяснений может быть то, что адреса кошельков распространяются в группах только для приглашений в WhatsApp и Signal для получения пожертвований от украинского ИТ-сообщества, проживающего за рубежом. Другая возможность может заключаться в том, что международные пожертвования в криптовалютах, поступающие в официальные кошельки украинского правительства в биткойнах, Thether и Etherium,

[116] Там же.

[117] HackenProof, «Призыв к эксплойтам. Остановим войну», 25 мая 2022 г., https://web.archive.org/web/20220525132844/https://hackenproof.com/ukraine-will- win/save-millions-lives-hackers-against-russia.

[118] HackenProof, «Призыв к эксплойтам. Остановим войну», 14 марта 2022 г., https://web.archive.org/web/20220314082410/https://hackenproof.com/ukraine-will-win/save-millions-lives-hackers-against-russia.

[119] Егор Аушев, Twitter, 27 февраля 2022 г., https://web.archive.org/web/20220509135052/https://twitter.com/Yegor_au/status/1497880962990059522.

[120] Tokenview, «Tether Explorer: THTCwoLQ4dg5uzLLPyaUSbB1x8rYKFAPA3», дата обращения – 8 июня, https://usdt.tokenview.com/en/address/THTCwoLQ4dg5uzLLPyaUSbB1x8rYKFAPA3.

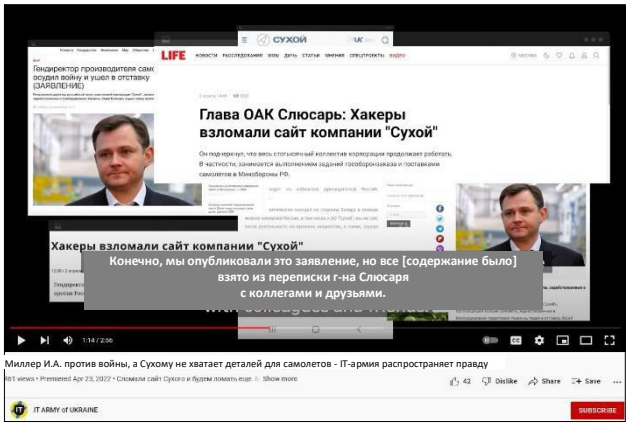
[121] Адам Янофски, «Эта украинская киберфирма предлагает хакерам вознаграждение за обрушение российских сайтов», *The Record*, 4 марта 2022 года, https://therecord.media/this-ukrainian-cyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites/ или https://archive.ph/38X95.

частично подкрепляют программу bug bounty Аушева.[122] По состоянию на 21 апреля ни Аушев, ни Cyber Unit Tech не объявляли о начале второй фазы своей программы bug bounty. Неизвестно, действительно ли программа выплачивала какие-либо вознаграждения и передавались ли кому-либо сообщения о выявленных уязвимостях. Учитывая близость Аушева к украинскому правительству и стратегическим партнерам Cyber Unit Tech, в число которых входит Совет национальной безопасности и обороны Украины, мы можем с некоторой долей уверенности сделать вывод, что сведения об уязвимостях могли оказаться в руках Министерства обороны Украины, спецслужб или IT-армии.

5 Непубличная структура и задачи

Помимо видимых общественности структур IT-армии и публикуемых задач, существует также собственное подразделение IT-армии.

Намеки на собственное подразделение впервые появились в начале марта, когда IT-армия взломала сайт miranda-media[.]ru, являющийся российским интернет-провайдером, обслуживающим Крымский полуостров.[123] Было еще несколько случаев взлома, ни один из которых не привлек широкого внимания средств массовой информации. Исключением являются 2 и 6 апреля, когда на взломанных сайтах Sukhoi[.]ru и Gazprom[.]ru были размещены фальшивые заявления Юрия Слюсаря (генерального директора «Сухого») и Алексея Миллера (генерального директора «Газпрома») с критикой Кремля за войну на Украине.[124] В то же время в обществе возникли сомнения, были ли веб-сайты взломаны неизвестной группой и соответствовали ли сделанные заявления действительности. Туман войны рассеялся три недели спустя, 23 апреля, когда канал IT-армии опубликовал трехминутное видео, в котором признал авторство ложных заявлений. Как поясняется в видео, «мы опубликовали это заявление, но все [содержание было] взято из переписки г-на Слюсаря с коллегами и друзьями. [...] В кремлевском окружении люди давно знают о позиции [Алексея Миллера]. Мы просто обнародовали ее, полностью собрав его мысли из переписки».[125] На момент написания этой статьи, как на канале IT-армии, так и в чате какие-либо обсуждения, касающиеся взломов, отсутствуют.



Скриншот видео IT-армии, опубликованного 23 апреля 2022 года на Youtube-канале IT-армии

4 апреля IT-армия опубликовала двухминутное видео об использовании Clearview на Украине для идентификации российских солдат.[126] Clearview – это скандальная компания по распознаванию лиц с использованием искусственного интеллекта со штаб-квартирой в США, которая собрала обширную биометрическую базу данных путем извлечения изображений лиц из социальных сетей и Интернета в целом, чтобы легко идентифицировать и определять местонахождение любого человека. В настоящее время компания сталкивается с несколькими судебными исками в США и была оштрафована различными надзорными органами за нарушение конфиденциальности в ЕС.[127] 23 мая Управление Комиссара по информации Великобритании оштрафовало Clearview более чем на 7,5 миллионов фунтов стерлингов и обязало компанию удалить все данные жителей Великобритании из своих систем.[128] Кашмир Хилл из The New York Times лучше всего объяснил влияние Clearview, заявив, что «поиск кого-либо по лицу может стать таким же простым, как поиск имени в Google. Незнакомые люди смогут подслушивать конфиденциальные разговоры, фотографировать участников и узнавать личные секреты.

[122] Кевин Рейнолдс, «Украинское правительство получает почти 10 миллионов долларов в виде криптовалют после российского вторжения», *CoinDesk*, 26 февраля 2022 г., https://www.coindesk.com/business/2022/02/26/ukrainian-government-is-seeking-crypto-donations/ или https://archive.ph/q5Yn3; Кристофер Роббинс, «Растущий спасательный круг цифровых активов на Украине», *CoinDesk*, 31 марта 2022 г., https://www.coindesk.com/markets/2022/03/31/the-growing-digital-asset-lifeline-in-ukraine/ или https://archive.ph/0pYX0.

[123] Штефан Соесанто, Twitter, 12 марта 2022 г., https://web.archive.org/web/20220608105346/https://twitter.com/iiyonite/status/1502658550937567232, Видео показывает взломанный веб-сайт на отметке: 0:15; https://www.youtube.com/watch?v=o4Wi5rFemro.

[124] Штефан Соесанто, Twitter, 24 апреля 2022 г., https://web.archive.org/web/20220608105316/https://twitter.com/iiyonite/status/1518189001819279360; «Веб-сайт российской нефтяной компании “Газпром нефть” “лег” после очевидного взлома», *Reuters*, 6 апреля 2022 г., http://web.archive.org/web/20220608151249/https://www.reuters.com/business/energy/russian-oil-company-gazprom-nefts-website-appears-have-been-hacked-2022-04-06/; Александр Щерба, Twitter, 2 апреля 2022 г., https://twitter.com/olex_scherba/status/1510185641547640832 или https://archive.ph/FCYL2.

[125] IT-армия Украины, Telegram-канал, 23 апреля 2022 г., https://t.me/itarmyofukraine2022/310 или https://archive.ph/c1UBk.

[126] IT-армия Украины, «IT-армия Украины: обращение к россиянам», Youtube, 4 апреля 2022 года, https://youtu.be/AYJSBSmLlnU; IT-армия Украины, Telegram-канал, 4 апреля 2022 г., https://t.me/itarmyofukraine2022/267 или https://archive.ph/e7eCI.

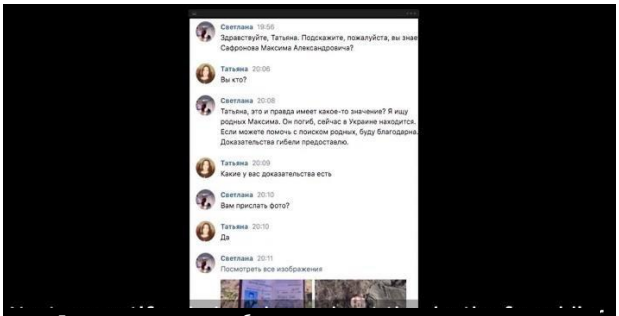
[127] Адам Швартц, «Победа! Против Clearview’s Face Surveillance возбуждается все больше и больше судебных исков», Фонд Electronic Frontier Foundation, 15 февраля 2022 г., http://web.archive.org/web/20220608151243/https://www.eff.org/deeplinks/2022/02/victory-another-lawsuit-proceeds-against-clearviews-face-surveillance; Privacy International, «Вызов ИИ Clearview в Европе», дата обращения – 8 июня, http://web.archive.org/web/20220608151333/https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe.

[128] ICO, «ICO оштрафовало компанию Clearview AI Inc, занимающуюся базой данных распознавания лиц, на сумму более 7,5 млн фунтов стерлингов и приказало удалить данные в Великобритании», ICO, 23 мая 2022 г., https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/.

Случайного прохожего на улице можно будет сразу идентифицировать, а его домашний адрес можно будет узнать всего лишь несколькими щелчками мыши. Этим будет положен конец публичной анонимности».[129]

13 марта агентство *Reuters* сообщило, что министерство обороны Украины начало использовать Clearview для идентификации погибших российских солдат.[130] Десять дней спустя министр цифровой трансформации Украины Михаил Федоров объяснил в Telegram, что «сегодня мы используем искусственный интеллект для поиска аккаунтов в социальных сетях мертвых российских солдат по фото трупов, чтобы сообщить об их смерти друзьям и родственникам и развеять миф о “спецоперации” в которой “нет призывников” и “никто не умирает”».[131] Точные данные об использовании Clearview на Украине было трудно получить, пока 4 апреля IT-армия не опубликовала свое видео. В нем IT-армия объяснила, что она использует Clearview для прямого контакта с семьями и близкими погибших солдат через социальные сети и приложения для обмена сообщениями, информируя их о смерти их родственника и прикрепляя фотографию изуродованного трупа и паспорт. В то время как многие западные СМИ продолжали описывать действия Украины как морально приемлемые и почти гуманитарные, следует серьезно задаться вопросом, будет ли столь же позитивно воспринята ситуация, в которой Исламское государство напрямую будет связываться с американскими семьями, отправляя им фотографии изуродованного трупа их родственника через социальные сети.[132] Утверждения о сугубо гуманитарно-пропагандистской природе этих действий откровенно игнорируют тотальную информационную войну, которую Украина ведет против российского общества в целом.

По данным IT-армии, по состоянию на 4 апреля украинское правительство успешно идентифицировало 582 трупа с помощью Clearview. Точная цифра, вероятно, была предоставлена IT-армии Министерством обороны Украины, украинскими разведывательными службами или министерством цифровой трансформации. Ни один из аспектов Clearview никогда не упоминался в канале или чате IT-армии.



Скриншот видео IT-армии, опубликованного 4 апреля 2022 года в Telegram-канале IT-армии

6 апреля IT-армия опубликовала четырехминутное видео, в котором показано, как они звонят семье российского солдата, который якобы украл около 100 килограммов товаров на Украине. Награбленное было отправлено по почте из почтового отделения в Мозыре, Беларусь, в город Чита на дальнем востоке России.[133] На видео IT-армии указан точный вес шести посылок, за которые заплатил солдат (общим весом около 100 кг), а также номер телефона и адрес получателя (брата солдата). На видео также показана запись с камер видеонаблюдения нескольких российских солдат с посылками в том же почтовом отделении. В начале телефонного разговора IT-армия грозит юридическими последствиями, выдавая себя за ФСБ. Звонок заканчивается словами IT-армии: «Мы знаем, где вы живете, где живет ваш брат, мы знаем все о вашей семье. Вы будете нести ответственность за каждое действие, которое вы совершили на территории Украины».[134]

Скриншот видео IT-армии, опубликованного 6 апреля 2022 года в Telegram-канале IT-армии

Впоследствии IT-армия опубликовала два аналогичных видеоролика 8 и 9 апреля. На первом из них русский солдат

[129] Кашмир Хилл, «Секретная компания, которая может положить конец конфиденциальности, какой мы ее знаем», The New York Times, 18 января 2020 года, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[130] Пареш Дейв и Джеффри Дастин, «Эксклюзивно: Украина начала использовать распознавание лиц с помощью ИИ Clearview во время войны», Reuters, 14 марта 2022 г., https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/.

[131] Михаил Федоров, Telegram-канал, 23 марта 2022 г., https://t.me/zedigital/1399 или https://archive.ph/focdY; Томас Брюстер, «Украина начинает использовать распознавание лиц для идентификации погибших россиян и информирования их родственников», *Forbes*, 23 марта 2022 года: https://www.forbes.com/sites/thomasbrewster/2022/03/23/ukraine-starts-using-facial-recognition-to-identify-dead- russians-and-tell-their-relatives/?sh=247648212898.

[132] Бен Гилберт (Ben Gilbert), «Украина использует технологию распознавания лиц для идентификации погибших российских солдат и информирования их семей», *Business Insider*, 24 марта 2022 г., https://www.businessinsider.com/ukraine-using-facial-recognition-tech-to-id-dead-russian-soldiers-2022-3?r=US&IR=T или https://archive.ph/3tjiA

[133] IT-армия Украины, Telegram-канал, 6 апреля 2022 года, https://t.me/itarmyofukraine2022/274 или https://archive.ph/4EQ2G.

[134] Там же.

посылает 16 кг из Мозырского почтового отделения своей жене в Новосибирск.[135] На втором видео другой российский солдат отправляет 63 кг своей жене в Хабаровск.[136] Видеозапись с камер видеонаблюдения одинакова во всех трех видеороликах, что позволяет предположить, что все три российских солдата посетили почтовое отделение в Мозыре вместе.

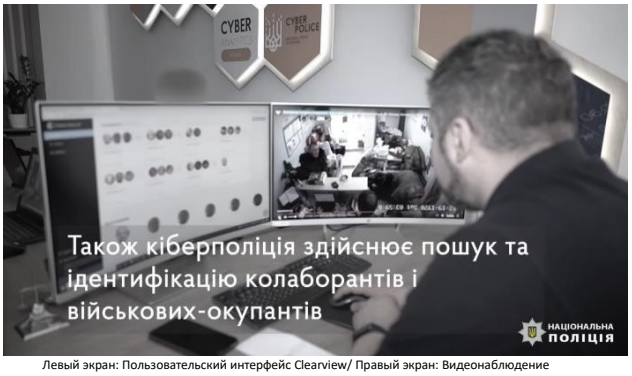
До сих пор неясно, как IT-армия смогла получить доступ к информации, необходимой для проведения такой операции. Откуда они узнали, каким именно белорусским почтовым отделением воспользуются эти российские солдаты? Взломали ли они камеру видеонаблюдения в почтовом отделении или запись была передана им другим агентством? На момент написания этой статьи ответов на эти вопросы нет, и ни одна из оперативных деталей звонков не обсуждалась на канале или в чате IT-армии.

Что мы знаем, так это то, что 2 июня 2022 года, через два месяца после того, как IT-армия опубликовала три видео, украинская киберполиция совместно со службой безопасности Украины (СБУ) использовала точные записи камер видеонаблюдения, чтобы объявить об идентификации 10 российских солдат Росгвардии из воинской части 6720 которые разграбили дома жителей в Буче, Украина.[137]

Фотография, опубликованная украинской киберполицией 2 июня 2022 г.

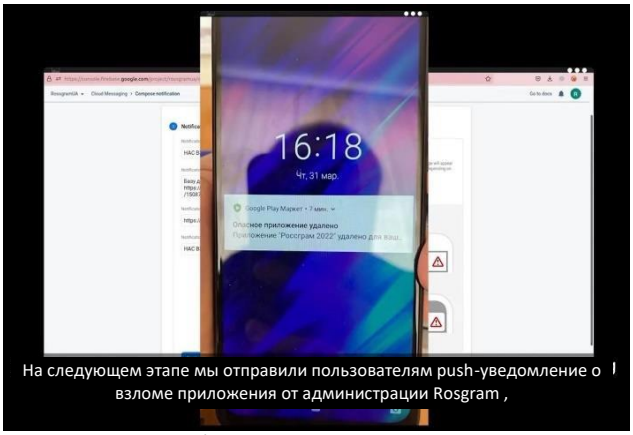
Хотя мы не знаем, кто первым получил в свои руки записи с камер видеонаблюдения или кто руководил этой операцией по сбору разведданных, мы можем сделать вывод, что либо IT-армия предоставила видеозапись киберполиции и СБУ, либо СБУ наблюдала за всей операцией и использовала как IT-армию, так и киберполицию для публикации пропагандистских материалов, опубликовав три призыва в апреле и объявив об идентификации солдат в июне. 16 июня

Национальная полиция Украины разместила на Youtube видео, в котором показано использование Clearview украинской полицией для идентификации российских солдат в почтовом отделении.[138]



Левый экран: Пользовательский интерфейс Clearview/ Правый экран: Видеонаблюдение с Мозырского почтового отделения

7 апреля IT-армия сообщила о своей самой хитроумной на сегодняшний день кампании, нацеленной на российский клон Instagram под названием Rossgram. До официального выпуска приложения Rossgram в конце марта IT-армия заявила, что (1) взломала базу данных регистрации для участия в бета-тестировании Rossgram, (2) создала поддельное приложение Rossgram, (3) разослала приглашения всем участникам бета-тестирования, (4) разослала всем, кто установил поддельное приложение, push-уведомления о том, что Rossgram был взломан, а затем (5) «слила» базу данных регистрации для участия в бета-тестировании в открытый доступ.[139] На сегодняшний день это единственная операция по взлому и сливу информации, за которую IT-армия взяла на себя прямую ответственность. Ничего из этого не обсуждалось в Telegram-канале и чате IT-армии.



Скриншот видео IT-армии, опубликованного 7 апреля 2022 года в Telegram-канале IT-армии

[135] IT-армия Украины, «Российские мародеры: Посылка в Хабаровск», Youtube, 8 апреля 2022 г., https://www.youtube.com/watch?v=yvH_TLXS4oY.

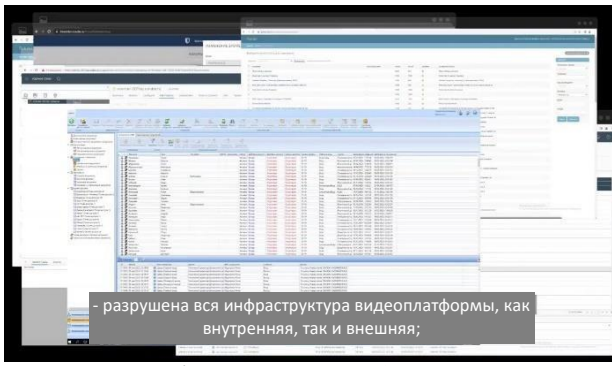
[136] IT-армия Украины, «Звонок российским мародерам: "Сувениры" из Украины?», Youtube, 9 апреля 2022 г., https://www.youtube.com/watch?v=lzdd4PVuETw.

[137] Киберполиция Украины, «Мародерили від білизни до побутової техніки: 10 російським армійцям оголошено підозри», cyberpolice.gov.ua, 2 июня 2022 года, https://cyberpolice.gov.ua/news/maroderyly-vid-bilyzny-do-pobu-tovoyi-texniky-rosijskym-armijczyam-ogolosheno-pidozry-1559/ или https://archive.ph/9R959; CyberpoliceUA, Telegram-канал, 2 июня 2022 г., https://t.me/cyberpolua/1379 или https://archive.ph/TVvRo.

[138] Национальная полиция Украины, «Протидія фейкам, пропаганді, хакерським атакам та шахрайству», Youtube, 16 июня 2022 г., https://www.youtube.com/watch?v=CxWn8dvONeg, временная отметка: 0:50-0:51

[139] «Россия представляет отечественного конкурента Instagram "Rossgram"», The Moscow Times, 29 марта 2022 г., https://web.archive.org/web/20220608133816/https://www.themoscowtimes.com/2022/03/29/russia-unveils-domestic-instagram-competitor-rossgram-a77123; IT-армия Украины, Telegram-канал, 7 апреля 2022 г., https://t.me/itarmyofukraine2022/276 или https://archive.ph/ZpMv7; Штефан Соесанто, Twitter, 7 апреля 2022 г., https://web.archive.org/web/20220608133944/https://twitter.com/iiyonite/status/1512001395255357443; Sudo rm -RF, Twitter, 29 марта 2022 г., https://web.archive.org/web/20220608133947/https://twitter.com/su-dormRF6/status/1508783518645735429.

14 мая IT-армия взяла на себя ответственность за подрывную кампанию против RuTube.[140] RuTube – российский конкурент Youtube, созданный еще в 2006 году. В середине марта аудитория RuTube начала стремительно расти, поскольку Youtube, в ответ на войну на Украине, фактически вытеснил российских создателей контента и пользователей со своей платформы, заблокировав рекламную систему Google в России.[141] Учитывая быстрый рост RuTube и значительное сокращение независимых СМИ в России, IT-армия определила RuTube как «главный информационный центр российской лживой пропаганды».[142] Ко дню празднованию Дня Победы в России 9 мая 2022 года, IT-армия с помощью «двух специалистов» провела подрывную кампанию против RuTube, начавшуюся в ночь на 8 мая. Согласно видео IT-армии, в ходе кампании были успешно (a) изменены все пароли администраторов, (б) заблокированы все карты доступа, которые были необходимы для входа и выхода из серверных комнат RuTube, (в) удалены «десятки петабайт информации», (г) «уничтожены все системы – виртуализация, базы данных, контент, конвертер, системы поиска контента, рекламный модуль, системы распределения нагрузки и управление всей инфраструктурой», и (е) похищена внутренняя информация на компьютерах администраторов и сотрудников RuTube.[143] Атака на RuTube – это первая в истории подрывная кампания, за которую IT-армия взяла на себя ответственность.



Скриншот видео IT-армии, опубликованного 14 мая 2022 года в Telegram-канале IT-армии

Доступ к RuTube отсутствовал почти три дня, и лишь 11 мая был восстановлен частично: Восстановление проходило поэтапно.[144] По данным официального Telegram-канала RuTube, российская компания по кибербезопасности Positive Technologies помогла расследовать и устранить последствия атаки.[145] RuTube также пояснил, что «на RUTUBE было совершено множество атак, которые были успешно локализованы. Однако инцидент 9 мая был другого уровня сложности. Готовность инфраструктуры к такой целенаправленной атаке может быть установлена только по результатам атаки».[146] 14 мая сайт, казалось, был полностью восстановлен из своих резервных копий.

На момент написания этой статьи все еще неизвестны ни размер группы собственных специалистов IT-армии, ни кто именно ставит перед ней задачи и предоставляет информацию. Группа собственных специалистов, вероятно, состоит из членов, проживающих на Украине, и украинцев, проживающих за рубежом. На момент написания этой статьи в IT-армии есть открытые вакансии для пентестеров, десктоп-разработчиков, хакеров, системных администраторов, графических дизайнеров и, самое главное, знатоков английского языка. На сайте вакансий задачи группы собственных специалистов описываются как «взлом вражеских ресурсов, распространение вирусов, создание фишинговых сайтов и нанесение максимального ущерба экономике и другим общественным сферам [России]».[147]

Любопытно, что 18 мая канал IT-армии опубликовал краудсорсинговый информационный призыв, в котором говорилось, что «нам нужна ваша помощь в поиске баз данных с номерами телефонов частных физических и юридических лиц из оккупированного Крыма, а также российских регионов рядом с украинской границей (Брянск, Курск, Белгород). Вы можете отправить эту информацию на адрес itarmyua@gmail[.]com».[148] Четыре дня спустя IT-армия поблагодарила всех, кто прислал информацию, и отправила второй запрос о помощи, заявив: «Нам нужна ваша помощь в поиске баз данных с номерами телефонов россиян, которые подпадают под одну из следующих категорий: (a) “молодые люди, имеющие радикальные взгляды и занимающиеся спортом (например, вышибалы, члены групп боевых искусств)”, (b) “призывники (люди, которые могут быть призваны на военную службу)”, (c) “студенты” и (d) “сотрудники военных служб и их родственники”»[149].

На момент написания этой статьи до сих пор неизвестно, с какой целью IT-армия собирала эту информацию. Эта информация может быть использована группой собственных специалистов в одной из предстоящих кампаний, она может быть опубликована в Интернете силами

[140] IT-армия Украины, Telegram-канал, 14 мая 2022 г., https://t.me/itarmyofukraine2022/349 или https://archive.ph/U0H43.

[141] Согласно Similarweb, «rutube.ru Ranking», дата обращения – 8 июня, https://www.similarweb.com/ru/website/rutube.ru/#overview; Справка – Youtube, «Информация для кандидатов на участие в Партнерской программе», дата обращения – 8 июня, https://support.google.com/youtube/answer/72851?hl=en&ref_topic=9153642.

[142] IT-армия Украины, Telegram-канал, 14 мая 2022 г., https://t.me/itarmyofukraine2022/349 или https://archive.ph/U0H43, временная метка: 00:29.

[143] IT-армия Украины, Telegram-канал, 14 мая 2022 г., https://t.me/itarmyofukraine2022/349 или https://archive.ph/U0H43, временная метка: 01:26-02:11; Sudo rm -RF, Twitter, 10 мая 2022 г., https://web.archive.org/web/20220608105911/https://twitter.com/sudormRF6/status/1524143579140083715.

[144] Rutube, Telegram-канал, 10 мая 2022 г., https://t.me/rutube/4177 или https://archive.ph/jBcEV; Rutube, Telegram-канал, 11 мая 2022 г., https://t.me/rutube/4180 или https://archive.ph/YcSeH; Rutube, Telegram-канал, 11 мая 2022 г., https://t.me/rutube/4181 или https://archive.ph/FSaUc.

[145] Rutube, Telegram-канал, 10 мая 2022 г., https://t.me/rutube/4179 или https://archive.ph/018cq; Rutube, Telegram-канал, 11 мая 2022 г., https://t.me/rutube/4180 или https://archive.ph/YcSeH.

[146] Rutube, Telegram-канал, 12 мая 2022 г., https://t.me/rutube/4183 или https://archive.ph/397ev.

[147] IT-армия Украины, веб-сайт, вакансии, дата обращения – 8 июня, https://web.archive.org/web/20220608134307/https://itarmy.com.ua/vacancies/?lang=en.

[148] IT-армия Украины, Telegram-канал, 18 мая 2022 г., https://t.me/itarmyofukraine2022/364 или https://archive.ph/KMKTj.

[149] IT-армия Украины, Telegram-канал, 22 мая 2022 г., https://t.me/itarmyofukraine2022/375 или https://archive.ph/LPpT0.

Украины для проведения информационных атак или организации россиян в России для проведения действий против российского государственного аппарата. Время покажет.

6 Где украинская разведка?

IT-армия является главным центром «наступательного» ответа Украины в киберпространстве на российское вторжение. Параллельно с этими кибератаками 28 февраля «Интернет-войска» Украины были мобилизованы для ведения национальной «наступательной» кампании в области информационной войны. В центре внимания Интернет-войск находится организация кампаний политического давления за рубежом и распространение украинской военной пропаганды через социальные сети, включая Telegram, VKontakte, Discord и Reddit. Министерство цифровой трансформации взяло на себя ответственность за создание как IT-армии, так и Интернет-войск Украины 10 марта.[150]

В нынешнем виде IT-армия и Интернет-войска публично изображаются как два правительственных проекта, возглавляемых гражданскими лицами, которые функционируют совершенно отдельно от структуры военного командования Украины и не поддерживают никаких связей с национальными разведывательными службами. Однако с чисто институциональной точки зрения весьма сомнительно, имеет ли Министерство цифровой трансформации законные полномочия самостоятельно создавать IT-армию и Интернет-войска без какой-либо координации или контроля со стороны служб обороны и разведки Украины. Решение украинских служб обороны и разведки сидеть сложа руки и позволить IT-армии и Интернет-войскам свободно и независимо проводить свои операции, особенно во время войны, кажется не только аналитической натяжкой, но и, весьма вероятно, приведет к стратегической путанице и вмешательству на тактическом уровне в собственные кибероперации служб обороны и разведки.

Также под вопросом остается наличие у Министерства цифровой трансформации необходимых собственных навыков и знаний, лежащих в основе кибер- и информационных атак, проводимых IT-армией и Интернет-войсками. В беседе с Антоном Мельником, который является советником Министерства цифровой трансформации, тот объяснил, что «мы реструктурировали Министерство цифровой трансформации в четкую военную организацию».[151] Точно так же, в интервью Politico 8 марта, заместитель министра цифровой трансформации Александр Борняков отметил, что «мы первые в мире, кто стал использовать в войне это новое оружие – мощное и одновременно простое. [...] Его работу невозможно нарушить или полностью подорвать».[152]

Еще в марте 2022 года Дина Темпл-Растон взяла интервью у одного из восьми администраторов канала IT-армии для *The Record*. Вероятно, самый интересный диалог состоялся в самом начале, когда Дина спросила: «У вас есть военное образование?» Администратор ответил: «Ну, типа того [...] Это не те вопросы, на которые я могу ответить вам полностью, потому что это может привести к большему пониманию того, кем я являюсь».[153] Хотя и не имея уверенности, мы можем лишь сделать некоторый вывод, что любое заявление о том, что ты служил на трех основных службах, еще не дает какого-либо полного понимания. Т.е., утверждение «Я служил на флоте» может означать что угодно – от повара до специалиста по подрывным работам на флоте. Но прямой отказ что-либо говорить может намекать на опыт работы в разведке. Точно так же крайне маловероятно, что случайному человеку, не прошедшему проверку в Интернете, доверят роль администратора канала IT-армии и надзор за сообществом, насчитывающим около 300 000 подписчиков, для организации «новой войны» Борнякова. Как минимум, можно было бы ожидать наличие у него некоторого опыта участия в кампаниях в социальных сетях или правительственной координации, а как максимум – разведывательного/ военного опыта в кибер- или информационной войне.

Интересно отметить, что с точки зрения России, IT-армия и Интернет-войска, вероятно, поддерживают тесные отношения с 72-м Центром информационно-психологических операций Украины в Броварах (Киевская область), или даже могут быть его ответвлениями. 72-й Центр был создан еще в 2003 году в Севастополе в составе Сил специальных операций Украины и был одним из последних воинских подразделений, которые сопротивлялись российской оккупации Крыма в 2014 году. До недавнего времени 72-й центр был главным центром Украины, специализирующимся на информационно-психологических операциях.[154] Очень мало публично известно о внутренней структуре и операциях, которые 72-й центр проводил в прошлом, а учитывая контекст текущей

[150] KMU.gov.ua, «Мінцифри бореться з ворогом на цифровому фронті», 10 марта 2022 г., https://web.archive.org/web/20220310141242/https://www.kmu.gov.ua/news/mincifri- boretsya-z-vorogom-na-cifrovomu-fronti.

[151] Саймонайт и Вольпичелли, «Минцифры Украины – это грозная военная машина».

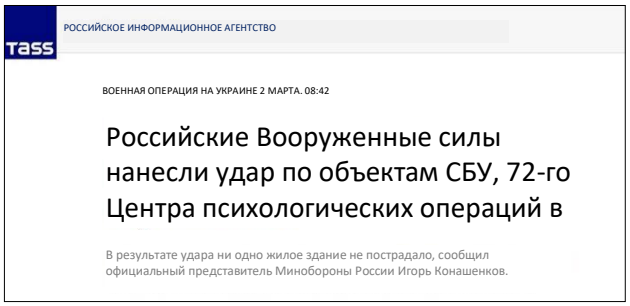
[152] Элиз Лабот, «"Мы первые в мире, кто стал использовать это новое оружие": Цифровая битва Украины против России», Politico, 8 марта 2022 г., https://web.archive.org/web/20220608135145/https://www.politico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber- social-media-00014880.

[153] Дина Темпл-Растон, «Борьба с Россией с помощью компьютеров, а не винтовок», *The Record*, 22 марта 2022 г., https://web.archive.org/web/20220608135214/https://therecord.media/fighting-russia-with-computers-not-rifles/.

[154] Есть также три небольших центра, специализирующихся на информационно-психологических операциях: 16-й центр базируется в Житомире, 74-й – во Львове и 83-й – в Одессе.

войны, довольно трудно отличить достоверную новую информацию от российской военной пропаганды.[155] Например, по данным Российского Совета по международным делам, 72-й центр не только участвует в разведывательной, вспомогательной и контрразведывательной деятельности, но и проводит «пропагандистские информационные кампании в сетях телекоммуникаций и Интернете, и совместно со [Службой безопасности Украины] координирует деятельность украинских патриотических хакерских групп, волонтерских информационных сообществ и интернет-ресурсов».[156]

Что мы точно знаем, так это то, что 1 марта Министерство обороны России заявило, что «информационные атаки на Россию осуществляются 72-м Главным центром информационно-психологических операций Вооруженных сил Украины совместно с подразделениями кибероперациий СБУ с использованием технических средств и программных систем и средств связи в Киеве».[157] Далее Министерство пояснило, что «для того чтобы сорвать информационные атаки против России, [российские силы] нанесут удары по технологическим объектам [Службы безопасности Украины] и 72-му главному [Психологические операции] центру в Киеве».[158] 2 марта российские авиаудары уничтожили штаб-квартиру СБУ, 72-й Центр, а также здание, в котором размещалась диспетчерская киевской телебашни. [159] Примечательно, что на момент написания этой статьи ни один российский авиаудар не был направлен на здание Министерства цифровой трансформации.



Источник: https://tass.com/defense/1414709

Еще одна часть головоломки, отчасти связанная с этим, появилась 7 марта, когда консультант по кибербезопасности Джеффри Карр опубликовал статью в своем блоге Inside Cyber Warfare, в которой утверждалось, что Белоярская атомная электростанция в Заречном, Россия, была взломана кибератаками из Главного управления разведки Министерства обороны Украины (ГУР МОУ). По словам Карра, ГУР МОУ похитило «большое количество данных, в том числе контракты, архитектурные схемы, конфигурации систем сигнализации, инструкции по настройке частей системы управления». [160] Однако весьма сомнительно, что Карр является надежным источником. Как он сам объясняет, «проблема была в том, что журналисты хотели говорить с ГУР МОУ, но об этом не могло быть и речи [...]. Они смогли поговорить со мной, т.к. я был единственным человеком, с которым команда ГУР МОУ могла общаться напрямую».[161] Учитывая непроверяемость заявлений Карра, журналисты по праву не хотели рисковать своей репутацией из-за информации, полученной из одного источника. На момент написания этой статьи Карр опубликовал еще 16 материалов, в которых утверждалось, что ГУР МОУ взломало «Роскосмос», «Газпром», службы связи Черноморского флота, а также Подразделение специальных операций 607 ФСБ. Ни одно из этих утверждений не было подтверждено. В начале апреля Карр зашел так далеко, что намекнул, что ГУР МОУ получило доступ к системам контроля давления газа «Газпрома», что якобы привело к физическому разрыву и пожару на двух российских трубопроводах.[162] Нет никаких доказательств, подтверждающих заявления Карра. Проблему усугубляет также тот факт, что Карр утверждает, что у него есть полная база данных, якобы похищенных ГУР МОУ, но доступ к ним разрешен только платным подписчикам. Почему он не обращается к DDoSecrets, как это часто делал Anonymous для слива данных? Почему ГУР МОУ использует только Карра в качестве своего общественного представителя и никого другого – ни IT-армию, ни Интернет-войска, ни кого-либо из хорошо подготовленных профессиональных журналистов, освещающих киберпространство? Учитывая отсутствие логических ответов, заявления Карра следует воспринимать с большой осторожностью. Тем не менее, отчет Карра действительно дает простой ответ на вопрос о том, чем

[155] См., например: Марина Совина, «В Крыму опровергли информацию о массовой мобилизации», *Lenta*, 26 марта 2022 г., https://lenta.ru/news/2022/03/26/krim/ или https://archive.ph/ddzNi; Spravdi.gov.ua, «Кровавая предосторожность генерала Мизинцева. Как работает российская пропаганда во время войны», 7 апреля 2022 г., https://spravdi.gov.ua/en/general-mizintsevs-bloody-precaution-how-russian-propaganda-works-during- the-war/.

[156] РСМД, «Организация кибербезопасности Украины», дата обращения – 8 июня, https://web.archive.org/web/20220608134819/https://russiancouncil.ru/cyber ukraine-org.

[157] Свобода, «Минобороны России анонсировало удары по объектам СБУ в Киеве», 1 марта 2022 г., https://www.svoboda.org/a/minoborony-rossii-anonsirovalo-udary-po-obektam-sbu-v-kieve/31730350.html. Обратите внимание, что 24 февраля, в первый день вторжения, российские новостные агентства предположили, что 72-й Центр подвергся первоначальному шквалу российских авиаударов. См.: РИА-Новости, «Очевидцы: в районе военных частей на окраине Киева поднимается дым», 24 февраля 2022 г., https://web.archive.org/web/20220608134747/https://ria.ru/20220224/dym-1774674819.html.

[158] ТАСС, «Минобороны России предупредило о готовящихся ударах по военным объектам в Киеве», 1 марта 2022 г., https://tass.ru/armiya-i-opk/13917097 или https://archive.ph/8x3nO.

[159] ТАСС, «В МО РФ сообщили, что аппаратная вещания телевышки в Киеве выведена из строя», 2 марта 2022 г., https://tass.ru/armiya-i-opk/13926529 или https://archive.ph/9vaqx. После авиаударов украинское правительство заявило, что мемориальный комплекс холокоста Бабий Яр также пострадал, что вызвало возмущение в западных СМИ и еврейских организациях. По словам корреспондента CNN по национальной безопасности Алекса Марквардта, по состоянию на 2 марта главный мемориал не пострадал (см.: https://web.archive.org/web/20220608134808/https://transcripts.cnn.com/show/nday/date/2022-03-02/segment/05).

[160] Джеффри Карр, «Российская Белоярская атомная электростанция была взломана киберподразделением ГУР МОУ», Inside Cyber Warfare, 7 марта 2022 г., https://web.archive.org/web/20220608110016/https://jeffreycarr.substack.com/p/russias-beloyarsk-nuclear-power-plant?s=r.

[161] Джеффри Карр, «Мой опыт работы с украинской наступательной киберкомандой», *O'Reilly*, 22 марта 2022 г., https://www.oreilly.com/radar/d-day-in-kyiv/ или https://archive.ph/gTd1x.

[162] Джеффри Карр, «Хакеры ГУР МОУ идут в атаку на Газпром – уже два пожара на трубопроводах», Inside Cyber Warfare, 5 апреля 2022 г., https://web.archive.org/web/20220608105903/https://jeffreycarr.substack.com/p/gurmo-hackers-go-kinetic-against?s=r.

украинские спецслужбы занимаются в киберпространстве. Если принимать статьи Карра за чистую монету, то ГУР МОУ в первую очередь фокусируется на операциях по взлому и сливу информации, которые оказывают еще меньшее непосредственное влияние на ход войны, чем те, которые проводились Anonymous и другими хакерскими группами с начала вторжения.[163] Аналогичным образом, если рассматривать стратегическое и общественное влияние, которое IT-армия и Интернет-войска оказали на российское общество, частные компании и иностранные правительства, то влияние ГУР МОУ практически ничтожно.

Отсутствие сведений о каких-либо действиях Cloud Atlas – единственной хакерской группе из списка APT (англ. advanced persistent threat – постоянная серьезная угроза) предположительно украинского происхождения – во время российского вторжения является еще одной загадкой, которая до сих пор не разгадана.[164] В целом, в настоящее время нет надежных сведений о том, что именно разведывательные и оборонные ведомства Украины делают в киберпространстве. Единственный логичный вывод, который можно сделать на основе доступной на сегодня информации, заключается в том, что украинские спецслужбы, вероятно, тесно связаны с постановкой задач и определением целей DDoS-атак, совершаемых IT-армией, информационными атаками Интернет-сил и операциями, проводимыми группой собственных специалистов IT-армии. Утверждения о том, что украинские спецслужбы и службы обороны вообще не причастны ни к одному из этих действий, являются либо наивными, либо – на данный момент – выдают в их авторе желание закрыть глаза на происходящее.

7 IT-армия и внешние группы

Исследователь разведки с открытым исходным кодом CyberKnow собрал наиболее полный обзор всех разных хакерских групп/ отдельных хакеров, которые появились после российского вторжения.[165] 1 мая CyberKnow выявила 74 активные группы/хакеров – 46 проукраинских, 26 пророссийских и две, чья принадлежность к какой-либо из сторон неизвестна.[166]

Помимо участия IT-армии в DDoS-атаках в сотрудничестве с различными группами в Telegram, очень мало известно о том, как IT-армия относится к таким группам, как «Белорусские киберпартизаны», и многочисленным подгруппам, действующим под знаменем Anonymous.

«Партизаны» были сформированы еще в сентябре 2020 года в ответ на протесты и последовавшие за ними жестокие репрессии после оспариваемых президентских выборов в Беларуси. Первой известной публичной акцией группы стал взлом веб-сайта белорусского президента 2 сентября 2020 года. Всего девять дней спустя «Партизаны» провели одну из своих самых результативных на сегодняшний день операций по взлому и сливу информации, обнародовав обширную базу данных сотрудников белорусских правоохранительных органов в NEXTA, которая стала крупнейшим русскоязычным Telegram-каналом/ СМИ, освещающим протесты в Беларуси. В августе 2021 года «Партизаны» стали одной из трех организаций-учредителей Альянса белорусского сопротивления «Супрацiў». Две других – это «Летящие аисты», ведущие активную деятельность за пределами киберпространства, и «Отряды самообороны», публикующие обучающие видеоролики и инструкции по самообороне. В контексте войны на Украине «Партизаны» получили международную известность, когда 24 января 2022 года они провели кампанию вымогательства против ИТ-систем белорусско-российских железных дорог, чтобы нарушить движение российских танков и техники.[167]

Anonymous

В отличие от «Партизан», Anonymous – это собирательное обозначения децентрализованных операций, складывающихся в глобальное движение Anonymous и его размытую идеологию.[168] После российского вторжения на Украину несколько известных информационных центров Anonymous в социальных сетях объявили о начале «Операции Россия» или #OpRussia.[169] В целом же каждая группа/хакер Anonymous проводит свои собственные операции. Иногда группы/хакеры Anonymous проводят условно совместные операции, а иногда даже могут атаковать

[163] Кевин Коллиер, «Хакеры наводняют Интернет файлами, по их словам, российских компаний», *NBC News*, 5 апреля 2022 г., https://web.archive.org/web/20220608110222/https://www.nbcnews.com/tech/security/hackers-flood-internet-say-are-russian-companies-files-rcna21853.

[164] Джо Словик, «Текущие события широкомасштабных кампаний: Переход от образцов к выявлению активности», *First,* 14 декабря 2020 г., https://web.archive.org/web/20220608110326/https://www.first.org/blog/20201214-Current_Events_to_Widespread_Campaigns; Джо Словик, «Постоянная дилемма Cloud Atlas», Domaintools, 25 февраля 2021 г., https://web.archive.org/web/20220608110234/https://www.domaintools.com/resources/blog/the-continuous-conundrum-of-cloud-atlas.

[165] Cyberknow, «Cyberknow», *Medium*, дата обращения – 8 июня, https://web.archive.org/web/20220608110420/https://cyberknow.medium.com/.

[166] Cyberknow, «Обновление 13. Российско-украинская война 2022 – Трекер хакерских групп. 1 мая, *Medium*, 1 мая 2022 г., https://web.archive.org/web/20220608110359/https://cyberknow.medium.com/update-13-2022-russia-ukraine-war-cyber-group-tracker-may-1-f0188bc96af3.

[167] Энди Гринберг, «Почему взлом Белорусской железной дороги знаменует собой первый случай атаки с целью вымогательства», Wired, 25 января 2022 г., https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/; Белорусские киберпартизаны, Twitter, 24 января 2022 г., https://web.archive.org/web/20220608110648/https://twitter.com/cpartisans/status/1485615555017117700.

[168] В июле 2015 года Бьелла Коулман метко описала метаморфозу Anonymous как «переход от неудачников-троллей к неудачникам-активистам». См.: Габриелла Коулман, «Хакер, фейкер, разоблачитель, шпион – Многоликий Anonymous», (Verso: New York, 2015), стр. 8.

[169] YourAnonNews, Twitter, 26 февраля 2022 г., https://web.archive.org/web/20220608110756/https://twitter.com/YourAnonNews/status/1497574730282541060; Anon2World, «Anonymous: “Операция Россия”», Youtube, 27 февраля 2022 г., https://www.youtube.com/watch?v=kcb2yudJ29c.

одну и ту же цель одновременно по чистому совпадению.[170] На момент написания этой статьи «Операции Россия» в основном состояла из DDoS-атак и операций по взлому и сливу информации, направленных против российских частных компаний и государственной цифровой инфраструктуры. Важно подчеркнуть, что у каждой группы/хакера Anonymous есть свои собственные политические мотивы и этические соображения. Иногда эти мотивы могут вызывать первоначальное одобрение с последующей серьезной негативной ответной реакцией со стороны других групп Anonymous, как случилось, когда хакер из группировки Anonymous, известный как I_am_Mr_Grey (около 8000 подписчиков в Twitter), объявил об операции «Падающая звезда» (Operation Falling Star) в начале апреля 2022 года. Mr_Grey, по сути, пригрозил, что Anonymous взломают спутники на орбите и заставят их упасть с неба. В удаленном твите с видео Грей заявил: «Уважаемый НАТО/ ООН/ Путин – сообщение для вас. Мы начинаем операцию “Падающая звезда”. Если Путин предпримет второе вторжение, а вы, НАТО/ООН, ничего не предпримете, это БУДЕТ ваша судьба».[171] Впоследствии Mr_Grey подвергся насмешкам и остракизму до такой степени, что он униженно извинился за свое поведение.

Первое, что следует отметить, – это то, что как белорусские киберпартизаны, так и почти все группы, действующие под флагом Anonymous, работают, главным образом, в Twitter. IT-армия, напротив, работает исключительно в Telegram. При этом самым близким к официальному представителю IT-армии в Твиттере является аккаунт под названием sudo rm -RF (@sudormRF6), который утверждает, что представляет «Украинский киберфронт»[172] Связь между sudo rm -RF и IT-армией осуществляется по меньшей мере через три точки передачи данных. Во-первых, sudo rm -RF опубликовала базу данных регистрации для участия в бета-тестировании Rossgram 29 марта 2022 года – за неделю до того, как IT-армия опубликовала свое видео о Rossgram с помощью файлообменного сервиса Mega[.]nz.[173] Во-вторых, sudo rm -RF опубликовала несколько скриншотов внутренних файлов, документов и исходный код RuTube 10 мая – за четыре дня до того, как IT-армия опубликовала свое видео о RuTube. [174] И, в-третьих, счетчик учетных записей sudo rm -RF появляется на восемь секунд в видеоролике IT-армии о RuTube, во время которого рассказчик обсуждает «последовательную публикацию [внутренних документов [RuTube] на сервисе обмена файлами Mega[.]nz».[175]

За исключением sudo rm -RF, все остальные аккаунты, которые утверждают, что представляют IT-армию Украины в Twitter, не являются ни аффилированными, ни официально одобренными IT-армией. Сюда входит аккаунт ITarmyUA с примерно 45 600 подписчиками, который многие участники движения Anonymous изображали как официальный аккаунт IT-армии в Twitter. На самом деле, почти каждый раз, когда Anonymous утверждают, что сотрудничали с IT-армией, они помечают аккаунт ITarmyUA в своих твитах.[176] Таким образом, когда 29 апреля Twitter приостановил работу ITarmyUA, тысячи пользователей Twitter восприняли это как акт против Украины и, по сути, как политическую цензуру.[177]

Для каждого, кто потрудился присмотреться повнимательнее, сразу станет очевидно, что ITArmyUA – это переименованный аккаунт, созданный еще в августе 2018 года, который изменил название и удалил все свои твиты до марта 2022 года. Никто в Telegram-канале IT-армии никогда не упоминал и не делал заявлений касательно блокировки аккаунта ITArmyUA в Twitter. Официальный сайт IT-армии не ссылается на аккаунт ITarmyUA, и ни Михаил Федоров, ни Министерство цифровой трансформации не подписаны на аккаунт ITarmyUA в Twitter.

Так как же возмущение Anonymous вписывается в общую картину? Глядя на динамику и возможные мотивы, весьма вероятно, что кто-то, идентифицирующий себя с движением Anonymous, изменил свой аккаунт, чтобы выдать себя за IT-армию в Twitter. Аккаунт ITarmyUA впоследствии был раскручен многочисленными аккаунтами Anonymous, чтобы получить огромное количество подписчиков в Twitter из ниоткуда. Затем учетная запись была использована для придания легитимности утверждениям о том, что Anonymous активно сотрудничал с IT-армией, и, как следствие, создания иллюзии, что украинское правительство одобряет действия Anonymous.

Отчаянная охота Anonymous за легитимностью и официальным признанием правительства даже привела к тому, что некоторые группы внедрили логотип Anonymous в копии официальных видеороликов IT-армии, а другие зашли так далеко, что провозгласили себя официальным международным подразделением

[170] Например, в середине апреля 2022 года три группы/хакера из группировки Anonymous (DepaixPorteur, NB65 и неизвестная группа Anonymous) одновременно атаковали сайт ССК «Газрегион». Все три отправили свои файлы «Газрегиона» в DDoSecrets для публикации. Как выразился DDoSecrets, «Три разных источника хакеров-активистов отправили файлы «Газрегиона» примерно в одно и то же время, с некоторыми пересечениями». См.: DDoSecrets, «Газрегион», дата обращения – 8 июня, https://ddosecrets.com/wiki/Gazregion.

[171] I_Am_Mr_Grey, Twitter, 6 April 2022, https://web.archive.org/web/20220406183036/https://twitter.com/IAmMrGrey2/status/1511769272833515524.

[172] Sudo rm -RF, Twitter, 2 марта 2022 г., https://web.archive.org/web/20220516124424/https://twitter.com/sudormRF6/status/1499117121040752641; Примечание: «sudo rm -rf /» – это команда Linux, которая, по сути, стирает всю вашу систему Linux», см.: Linux Stans, «sudo rm -rf /: команда, которую вы никогда не должны выполнять», 19 февраля 2022 г., https://linuxstans.com/sudo-rm-rf /.

[173] Sudo rm -RF, Twitter, 29 марта 2022 г., https://web.archive.org/web/20220329123018/https://twitter.com/sudormRF6/status/1508783518645735429.

[174] Sudo rm -RF, Twitter, 10 мая 2022 г., https://web.archive.org/web/20220608111028/https://twitter.com/sudormRF6/status/1524143588019421184.

[175] IT-армия Украины, Telegram-канал, 14 мая 2022 г., https://t.me/itarmyofukraine2022/349 или https://archive.ph/U0H43, временная метка: 02:27-02:35.

[176] PucksReturn, Twitter, 28 апреля 2022 г., https://web.archive.org/web/20220608110810/https://twitter.com/PucksReturn/status/1519495471647047680.

[177] PucksReturn, Twitter, 29 апреля 2022 г., https://web.archive.org/web/20220608111103/https://twitster.com/PucksReturn/status/1520082201093804032; AnonOPsSE, Twitter, 30 апреля 2022 г., https://web.archive.org/web/20220608110953/https://twitter.com/AnonOpsSE/status/1520361102323953665.

IT-армии Украины.[178] Ни одно из этих утверждений никогда не было признано IT-армией. На самом деле, Telegram-канал IT-армии только один раз использовал слово «anonymous», когда 4 апреля опубликовал благодарность Telegram-группе Anonymous-Ukraine за сотрудничество DDoS-атаках.

В целом, не похоже, чтобы IT-армия была заинтересована в официальном признании какой-либо близости с движением Anonymous. Такое поведение, вероятно, связано с (a) децентрализованной природой Anonymous и незнанием того, кто говорит от чьего имени, и (б) общей неуправляемостью и непредсказуемостью Anonymous, где каждая группа и хакер делают то, что хотят, ради влияния в социальных сетях и привлечения общественного внимания. На момент написания этой статьи неизвестно, сотрудничала ли группа собственных специалистов IT-армии с группами, близкими к Anonymous. Неоднократные запросы по электронной почте в IT-армию для проверки заявлений, сделанных несколькими группами (включая BeeHiveCybersec), остались без ответа.

Белорусские киберпартизаны

Любопытно, что «Белорусские киберпартизаны» столкнулись со стороны IT-армии с такой же невосприимчивостью. 18 марта «Партизаны» написали в Твиттере, о том, что «[мы] готовы поддержать [IT-армию] разведданными, инструментами и операциями. Мы отправили им электронное письмо, а затем твитнули по этому поводу. Ответа от них мы пока не получили».[179] На повторный вопрос от 29 апреля «Партизаны» ответили, что «[мы] к сожалению, не смогли установить прямой контакт».[180] На момент написания этой статьи «Партизаны», по-видимому, так и не смогли связаться с IT-армией.

IT-армия действительно атаковала белорусские сайты 27 февраля, когда канал объявил о DDoS-атаке на 43 различных сайта, включая сайты белорусского правительства, СМИ, банков и промышленных компаний.[181] Две других подобных атаки произошли 20 марта – против белорусского сайта Bitrix24, компании по управлению взаимоотношениями с облачными клиентами, штаб-квартира которой находится в Вирджинии, США.[182] А 5 апреля IT-армия атаковала cdek[.]by – белорусский сайт российской международной компании экспресс-доставки СДЭК.[183]

С 5 апреля ни один белорусский сайт не был атакован IT-армией. Неясно, является ли это изменение преднамеренным ограничением, основанным на внутренних решениях, или просто эволюционным процессом, в результате которого IT-армия сосредоточилась исключительно на России.

Нежелание IT-армии общаться с «Партизанами», возможно, следует той же логике, что и в отношении Anonymous. У IT-армии нет ответов на такие вопросы как: (a) кто конкретно те люди, которые составляют группу «Партизан»; (б) может ли IT-армия доверять им; (в) каковы основные политические мотивы «Партизан», учитывая, что они являются частью Альянса белорусского сопротивления «Супраціў»; (d) может ли сотрудничество IT-армии и «Партизан» в киберпространстве политически рассматриваться как сотрудничество украинского правительства с белорусской оппозицией в изгнании; и (e) каковы варианты действий IT-армии, если действия «Партизан» пойдут не по ее сценарию.

В целом, гибридная система, освоенная IT-армией, требует здорового чувства паранойи и необходимости чрезвычайно серьезного отношения к оперативной безопасности для защиты от российских проникновений и утечек информации. Различать друзей, врагов и всех, кто между, – принципиально сложная задача, особенно во время войны.

IPStress

Одно любопытное внешнее сотрудничество обнаружилось в начале мая, когда itarmy[.]com].[ua] начал показывать своего единственного партнера в нижней части своего сайта: IPStress[.]in.[184] По сведениям от самого IPStress, он является лучшим IP-загрузчиком, который «может отключить любой игровой сервер, такой как ovh, nfo, серверы fivem и т.д. Мы обходим все средства защиты, такие как cloudflare, с помощью своих невероятно быстрых методов. Покупайте сейчас и наслаждайтесь огромной мощью наших ботнетов».[185] Это самоописание стало казаться несколько странным, после того как в начале 2022 года веб-сайт IPStress[.]in стал использовать службу защиты от DDoS-атак Cloudflare.[186]

[178] Anonymous, «Сообщение от IT-армии Украины и Anonymous», Youtube, 25 апреля 2022 года, https://www.youtube.com/watch?v=IfNf336Y5lY; WhiteDeathCyber, Twitter, 18 апреля 2022 г., https://web.archive.org/web/20220608111544/https://twitter.com/WhiteDeathCyber/status/1516010603843837957.

[179] Белорусские киберпартизаны, Twitter, 18 марта 2022 г., https://web.archive.org/web/20220608111705/https://twitter.com/cpartisans/status/1504801050444058624.

[180] Белорусские киберпартизаны, Twitter, 29 апреля 2022 г., https://web.archive.org/web/20220608111733/https://twitter.com/cpartisans/status/1520150809912266759.

[181] IT-армия Украины, Telegram-канал, 27 февраля 2022 года, https://t.me/itarmyofukraine2022/27 или https://archive.ph/xtC1p.

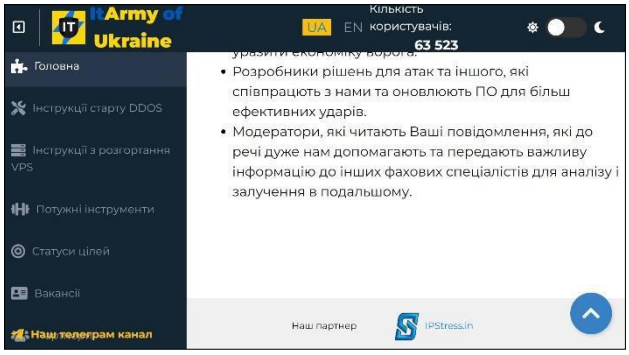
[182] IT-армия Украины, Telegram-канал, 20 марта 2022 г., https://t.me/itarmyofukraine2022/221 или https://archive.ph/sHfGY.

[183] IT-армия Украины, Telegram-канал, 5 апреля 2022 г., https://t.me/itarmyofukraine2022/269 или https://archive.ph/Tne61.

[184] IT-армия Украины, 9 мая 2022 г., https://web.archive.org/web/20220509132136/https://itarmy.com.ua/.

[185] IPStress, 19 декабря 2021 г., https://web.archive.org/web/20211219144712/https://ipstress.in/.

[186] IPStress, 31 мая 2022 г., https://web.archive.org/web/20220331084353/http://ipstress.in/.



Скриншот it army[.]com[.]ua от 9 мая 2022 г.

31 мая 2022 года ФБР и Министерство юстиции США объявили об аресте трех интернет-доменов: weleakinfo[.]to, ovhbooter[.]com и ipstress[.]in. В пресс-релизе Министерства юстиции США прокурор округа Колумбия Мэттью М. Грейвз объяснил, что ipstress и ovhbooter «публично предлагали проводить атаки типа “Распределенный отказ в обслуживании” или “DDoS” для клиентов – в частности, формат, называемый загрузочными или стрессорными атаками. […] Изъятие этих доменов было частью действий, скоординированных правоохранительными органами с Национальным полицейским корпусом Нидерландов и Федеральной полицией Бельгии. Действия, предпринятые нашими международными партнерами, включали арест основного субъекта, обыски в нескольких местах и изъятие инфраструктуры веб-сервера».[187]

Одновременно проходили захват всех трех доменов и облавы в нескольких местах, а это наводит на мысль о том, что это была кульминация длившегося несколько месяцев, если не год, уголовного расследования. Таким образом, ликвидация IPStress[.]in произошла не в связи с их партнерством с IT-армией. Тем не менее, вызывает беспокойство тот факт, что IT-армия – созданная правительством Украины организация – была готова установить и открыто рекламировать свое партнерство с киберпреступным DDoS-предприятием. На момент написания этой статьи сайт IT-армии сменил своего официального партнера на хостинг-сервис ukraine[.]com[.]ua.

Скриншот ipstress[.]in от 2 июня 2022 года

По состоянию на 7 июня 2022 года IPStress[.]in по-прежнему упоминается на веб-сайте IT-армии в официальном переводе на английский язык раздела «Друзья и партнеры IT-армии Украины».[188]

10 июня Министерство иностранных дел России заявило, что «по мнению экспертов, для проведения массированных DDoS-атак с участием “киберволонтеров” злоумышленники используют вредоносное программное обеспечение, расположенное на серверах компаний-поставщиков Hetzner (Германия) и DigitalOcean (США). Активно используются иностранные специализированные платформы (War.Apexi.Tech, Ban-Dera.com), регулярно используются онлайновые возможности IPstress.in и серверы Google».[189]

8 Заключение

IT-армия Украины – это уникальная и интеллектуальная конструкция, организационная структура и оперативное воздействие которой, вероятно, будут влиять на искусство кибер- и информационных войны в будущем. С публичной точки зрения, IT-армия служит механизмом, который позволяет украинскому правительству использовать добровольцев со всего мира в своих постоянных DDoS-атаках на российские правительственные и корпоративные веб-сайты. По состоянию на 7 июня 2022 года она имеет 662 цели. Что касается непубличной стороны, то группа собственных специалистов IT-армии, вероятно, поддерживает глубокие связи с украинскими службами обороны и разведки или в значительной степени состоит из них.

В целом, как Киев, так и украинское ИТ-сообщество в целом показали миру, как выглядит цифровая дипломатия на стероидах. Их поведение обрушило столпы существующих правовых норм и правил поведения государства в киберпространстве, и разрушило иллюзию отделения обороны Украины от украинских компаний и граждан, проживающих за рубежом. Точно так же, на момент написания этой статьи страны ЕС и НАТО пока не сумели адаптироваться или даже понять, что такое IT-армия на самом деле. Западные наблюдатели и правительства по-прежнему считают, что это всего лишь группа случайных добровольцев, проводящих бессмысленные DDoS-атаки на российские сайты. Они до сих пор не в состоянии разглядеть базовую организационную структуру, операционное поведение и широкую экосистему, которая лежит в основе борьбы IT-армии и Украины в кибер- и информационном пространстве. Хорошо это или плохо, но продолжающееся игнорирование сути IT-армии окажет разрушительное

[187] Министерство юстиции США, «WeLeakInfo.to и связанные с ним доменные имена изъяты», 31 мая 2022 г., https://www.justice.gov/usao-dc/pr/weleakinfoto- and-related-domain-names-seized или https://archive.ph/X5wAe.

[188] IT-армия Украины, «Друзья и партнеры IT-армии Украины», itarmy.com.ua, 7 июня 2022 г., https://web.archive.org/web/20220607134600/https://itarmy.com.ua/partners/?lang=en.

[189] Министерство иностранных дел Российской Федерации, «Ответ Специального представителя Президента Российской Федерации по международному сотрудничеству в области информационной безопасности, директора Департамента международной информационной безопасности Министерства иностранных дел России А.В. Крутских на вопрос СМИ об атаках на российскую критическую инфраструктуру» 9 июня 2022 г., https://www.mid.ru/ru/foreign_policy/news/1817019/ или https://archive.ph/8U6CN.

влияние на будущую стабильность киберпространства, а вместе с ним и ландшафт национальной безопасности в Европе и за ее пределами.

Есть много вопросов, которые этот отчет оставляет без ответа или на которые можно ответить только с разной степенью уверенности. Время покажет, как будет развиваться IT-армия в дальнейшем и будет ли история оценивать этот отчет как сбалансированный и объективный.

Некоторые вопросы, не затронутые в этом отчете, могут представлять интерес для будущих исследований и политических дискуссий, включая:

(1) Как это возможно, что официальный сайт IT-армии (itarmy[.]com[.]ua) и Cyber Palyanits (cyberarmy[.]com.ua) оказываются защищены от DDoS-атак службой Cloudflare? На обоих сайтах пользователи могут найти широкий ассортимент инструментов и инструкций для DDoS-атак. Кажется довольно странным, что такой anti-DDoS сервис, как Cloudflare, защищает те самые сайты, которые организуют наиболее эффективные DDoS-атаки во время войны на Украине.

(2) Как такое возможно, что официальная учетная запись электронной почты IT-армии и формы заявок размещены в Google, когда сайт itarmy[.]com[.]ua содержит подробные инструкции о том, как использовать облачные серверы Google для DDoS-атак?[190] Существует ли у Google политика в отношении воюющих сторон, использующих ее продукты в контексте международного вооруженного конфликта?

(3) Есть ли у GitHub, и, соответственно, у Microsoft политика удаления репозиториев/ инструментов, специально предназначенных для привлечения пользователей со всего мира к участию в международном вооруженном конфликте? На момент написания этой статьи высокопоставленные руководители Microsoft публично выступали против кибервойны, одновременно активно помогая Украине защищать свои сети, однако ни один из репозиториев GitHub, упомянутых в этом отчете, похоже, не нарушает условия предоставления услуг GitHub.

(4) Какова экономика IT-армии и экосистемы вокруг нее? Являются ли пожертвования в криптовалюте, поддержка инфлюэнсеров и держатели различных токенов Hacken основным источником дохода для улучшения DDoS-инфраструктуры IT-армии как на Украине, так и за ее пределами?

(5) И какие политические предпосылки создают американские компании-разработчики программного обеспечения, такие как Clearview, Starlink и, возможно, вскоре Palantir, предлагая свои новые технологии и инфраструктуру одной из сторон международного вооруженного конфликта? В контексте войны на Украине руководителям компаний может оказаться легко решить, какую из сторон поддерживать. Но что произойдет, когда это решение пойдет вразрез с внешнеполитическими интересами США? Кроме того, как другие правительства, особенно европейские, должны относиться к поведению этих компаний? Следует ли их рассматривать как продолжение внешней политики США? Или же они являются независимыми субъектами? И если да, то какие стратегические интересы, внешняя политика, а также правовые и этические соображения лежат в основе поведения этих компаний?

[190] IT-армия Украины, «Инструкции по развертыванию виртуальных машин», itarmy.com.ua, 7 июня 2022 г., https://web.archive.org/web/20220607144831/https://itarmy.com.ua/vps/.

Список сокращений

AF	Словарь «Urban dictionary»: «Сокращение от “as fuck”, используется с прилагательным, чтобы продемонстрировать максимальную степень чего-либо или кого-либо»
APT	(англ. Advanced Persistent Threat) – Постоянная серьезная угроза
AWS	(англ. Amazon Web Services) – Веб-службы Amazon
CCTV	(англ. Closed-Circuit Television) – кабельное телевидение
CET	(англ. Central European Time) – центральноевропейское время
СНГ	Союз независимых государств
CSS	(англ. Center for Security Studies) – Центр исследований кибербезопасности
Db1000n	(англ. Death by 1000 needles) – Смерть от 1000 игл
DDoS	(англ. Distributed Denial of Service) – Распределенный отказ в обслуживании
DNS	(англ. Domain Name Service) – Служба доменных имен
ЕГАИС	Единая государственная автоматизированная информационная система учета объема производства и оборота этилового спирта, алкогольной и спиртсодержащей продукции
ФСБ	Федеральная служба безопасности Российской Федерации
ГУР МОУ	Главное управление разведки Министерства обороны Украины
http	(англ. Hypertext Transfer Protocol) – Протокол передачи гипертекста
https	(англ. Hypertext Transfer Protocol Secure) – Безопасный протокол передачи гипертекста
IP	(англ. Internet Protocol) – Интернет-протокол
ISP	(англ. Internet Service Provider) – Интернет-провайдер
ИТ	Информационные технологии
LFI	(англ. Local File Execution) – Выполнение локального файла
NFT	(англ. Non-fungible Token) – Невзаимозаменяемый токен
НПО	Неправительственная организация
ОС	Операционная система
R&D	(англ. Research and Development) – Исследования и разработки
RCE	(англ. Remote Code Execution) – Удаленное выполнение кода
RFI	(англ. Remote File Execution) – Удаленное выполнение файлов
РСМД	Российский совет по международным делам
СБУ	Служба безопасности Украины
SCADA	(англ. Supervisory Control and Data Acquisition) – Диспетчерский контроль и сбор данных
SQLi	(англ. Structured Query Language (SQL) Injection) – Внедрение языка структурированных запросов (SQL)
Sudo rm -RF /	Команда Linux, которая, по сути, стирает всю систему
TGstat	Каталог Telegram-каналов и чатов Telegram Stat
UA	Украина
UDP	(англ. User Datagram Protocol) – Протокол пользовательских дейтаграмм
URL	(англ. Uniform Resource Locator) – Единый локатор ресурсов
VPN	(англ. Virtual Private Network) – Виртуальная частная сеть

Об авторе

Штефан Соесанто является старшим научным сотрудником Проекта по киберзащите Группы риска и устойчивости Центра исследований безопасности (CSS) в Швейцарской высшей технической школе Цюриха (ETH). Штефан тесно сотрудничает с Министерством обороны Швейцарии. Среди прочего, его работы публиковались Cyber Defense Review, Air University, Lawfare, Королевским институтом Элькано, Фондом Конрада Аденауэра, Defense One и Советом по международным отношениям.

CSS
ETH Zürich

Центр исследований безопасности (CS) в Швейцарской высшей технической школе Цюриха (ETH Zürich) является центром компетенций в области швейцарской и международной политики безопасности. Он предлагает экспертные знания по безопасности в области исследований, преподавания и консультирования. CSS способствует пониманию проблем политики безопасности и этим вносит свой вклад в борьбу за мир во всем мире. Его деятельность независима, актуальна для практики и основана на прочной научной основе.