Локализация Интернета как минимальная защита от интернет-оружия

Д-р Джордж Костопулос
Профессор кибербезопасности
Университет Университета Мэриленда, США

Введение

В последние годы в мире появился новый ресурс, который значительно расширил связь, что в равной степени повысило производительность практически всех секторов. Этот ресурс охватывает мир, как солнце и луну, став инфраструктурой для создания и реализации ранее невозможных достижений. Этот ресурс - это сеть Интернет - централизованная сеть сетей - это ценный актив за пределами количественной оценки.

Естественный вопрос: кто владеет Интернетом? «Интернет - это сеть сетей. Каждая из отдельных сетей принадлежит различным компаниям и организациям, и они полагаются на физические серверы в разных странах с различными законами и правилами ». [1]

Интернет номинально управляется и управляется ICANN (Internet Corporation для присвоенных имен и номеров) [2]. ICANN ". , , является некоммерческой организацией, ответственной за координацию обслуживания и процедур нескольких баз данных, связанных с пространствами имен и числовыми пространствами Интернета, обеспечивая стабильную и безопасную работу сети ». [3] Физические узлы расположены в странах по всему миру, что облегчает быстрое и эффективные операции. [4]

Это факт, что в Интернете, концептуально, нет никаких физических границ, и что мир полностью взаимосвязан с неограниченными преимуществами, которые должны быть получены. По мере того, как Интернет растет в своей полезности и охвате, это добросовестное предположение подрывается мыслью о потенциальных действиях, которые будут изолировать или разделить мир. Мир, который Интернет каким-то образом объединил.

В действительности, " . , , Интернет - сеть сетей. , , "[1]. Эти сети, состоящие из маршрутизаторов и серверов, мили кабелей - оптических и медных, а также беспроводных линий связи. Они принадлежат различным компаниям или национальным организациям, где они должны соблюдать правила и решения правительств соответствующих стран. Опасения перед Глобальной комиссией по управлению Интернетом состоят в том, что ". , , политический контроль, введенный правительствами, заставит людей потерять доверие к Интернету. , , [5] Как описано ниже в этой статье, существует множество случаев, когда правительства закрывают Интернет в отдельных районах и в определенные моменты, предположительно, для общего блага.

Несомненно, что большинство данных Western World физически находятся на серверах, расположенных в Соединенных Штатах. Различные организации социальных сетей, которые пользуются всемирным доверием и предлагают бесплатные услуги, имеют свои хранилища данных с миллиардами счетов в США. Университеты для их удобства имеют свои учетные записи электронной почты, управляемые gmail, которая является американской бизнес-организацией. Даже министерство иностранных дел европейской страны, после серьезного сбоя электронной почты, по неизвестной причине, теперь использует службы gmail. То есть, все электронные письма министерства хранятся на серверах gmail за тысячи километров.

В идеальном мире нет ничего плохого во всем вышеизложенном, но в современном мире правительства могут получить доступ ко всем учетным записям и данным всех серверов, маршрутизаторов и хранилищ данных, физически проживающих на их территориях. Кроме того, правительства могут обязать определенные компании не принимать учетную запись электронной почты клиента, если соответствующий сервер недоступен для них.

Пример реальной жизни - это то, что недавно в США американская леди хотела открыть банковский счет. Среди различных необходимых личных данных леди попросили войти в ее учетную запись электронной почты. Поскольку ее учетной записью была @ yandex.com, компания, у которой есть свои серверы за пределами США, ей было отказано в открытии банковского счета.

Мы слышим право и налево от американских санкций против других стран [6]. Что делать, если такие санкции включают в себя отключение интернет-коммуникаций в США и из США? Затем Интернет превратится из ценного актива в опасную ответственность.

Цель этой статьи состоит в том, чтобы поднять опасения, что Интернет постепенно становится политико-экономическим оружием и что только локализация в Интернете может минимизировать неблагоприятное воздействие такого интернет-вооружения. Через план локализации Интернета данные будут храниться, а услуги будут предоставляться из организаций, физически расположенных в стране клиентов, вместе с системами хранения данных.

Интернет-использование

Существуют бесконечные примеры, когда Интернет использовался в качестве информации или среды для дезинформации. Верят что " . , , Интернет играет большую роль в управлении, кампаниях и активизме. , , [7] Действительно, правительства очень эффективно используют Интернет, чтобы граждане знали различные законы, правила и положения. Однако, когда дело доходит до политических кампаний, «в 2008 году контент, созданный избирателями в социальных сетях, несколько раз менял траекторию кампании» [8].

К сожалению, помимо знаний и информации, Интернет служит в качестве громкоговорителя для ложных новостей. Однако такие новости достигают разных групп населения по разным ставкам. В то время как западная сторона Атлантики была затоплена ложными новостями, обвиняющими русских ». , , пытается вмешаться в

последние президентские выборы (США). , «[9] на восточной стороне Атлантики». , , большинство ложных новостей. , , достигнуто (только) 1 процент или меньше. , , онлайн-популяции. , , «[9]

К настоящему времени должно быть осознано, что Интернет стал неотъемлемой частью технологически развитого мира, и его разрушение создаст немыслимый и непоправимый ущерб. Вклад Интернета в бизнес и в экономику в целом является фундаментальным, и он создал очень ценную платформу. В секторе образования, где информация и знания постоянно поступают, любое нарушение интернет-услуг будет катастрофическим. Что касается индустрии здравоохранения, то ". , , Интернет является незаменимым коммунальным сервисом для индустрии здравоохранения. Большинство репозиториев информации, документации и записей пациентов хранятся на онлайн-серверах. »[10], и любые отключенные интернет-услуги будут эффективно закрывать больницы.

Завершение работы в Интернете

Сообщается, что «правительства во всем мире все чаще прибегают к отключению Интернета. , , с целью контроля обмена информацией в Интернете ». [11]. Отключение доступа к Интернету стало стандартной практикой в Индии по целому ряду причин: от предотвращения беспорядков до отказа от обмана в академических экзаменах [11]. По этой причине правительство Алжира, как и Ирак, отключило свой Интернет в течение ограниченного периода времени [13]. Во время так называемой арабской весны ». , , Египет предпринял беспрецедентный шаг по разрыву всех подключений к Интернету и прекращению обслуживания своих мобильных телефонов. , , »[13]. Кроме того, в России Интернет был отключен в Крыму, чтобы предотвратить ». , , предполагаемый террористический акт, который Украина нанесла в этом регионе. , , »[14].

Помимо государственных санкционированных интернет-отключений, также часто случаются анонимные отключения доступа к Интернету, ориентированные на конкретные сайты. Такие закрытости создаются за счет чрезмерного искусственного спроса на услуги на определенных веб-сайтах. Одна такая атака, известная как DDoS, Distributed Denial of Service, состоялась в США 21 октября 2016 года.

Эта атака отключила несколько популярных веб-сайтов, включая «. , , Vox, Twitter, Spotify, Amazon, PayPal и Reddit. , , что перегруженные веб-сайты, отправив им более 150 000 запросов на информацию в секунду.«[15] Некоторые аналитики разведки помчались, сказав это». , , их анализ указывает на Россию. , , и другие, говорящие, что это может быть просто «интернет-вандализмом». [15] В любом случае атака доказала уязвимость Интернета. Тем не менее, всегда можно определить, были ли эти атаки DDoS насыщенными атакованными серверами или насыщены узлами Интернета, которые были связаны с этими серверами. Конечно, нужно понимать, что невозможно спроектировать и построить сетевую систему с бесконечной пропускной способностью. Кроме того, следует признать, что нет абсолютного способа явно идентифицировать человека или организацию, находящуюся под кибератакой.

Интернет-оружие

Неизвестно, когда Интернет стал оружием разрушения. В большинстве случаев абсолютно невозможно идентифицировать злоумышленника. Можно только догадываться, основываясь на потенциальном получателе любых полученных преимуществ.

Однако некоторые из ранних вооружений Интернета включают в себя пресловутый Stuxnet. Это мощная вредоносная программа ». , , который, как полагают, является совместно построенным американским / израильским кибергламом ». [16], который появился в 2010 году и был разработан для атаки программируемых промышленных контроллеров, которые подвергаются воздействию Интернета. Еще одним ранним вредоносным ПО было Любовное письмо. «Этот червь отправляет себя на адреса электронной почты. , , перезаписывает файлы на локальных и удаленных дисках. , , уничтожая исходное содержимое. «[17] Считается, что основные державы этого мира поддерживают такой арсенал кибернетического оружия, который будет запущен по мере необходимости. У США в своем арсенале санкций есть программа санкций, связанная с кибер-связью, в которой излагаются ". , , связанные с кибер-активностью, подлежащие санкциям ». [18] Существует даже набор правил санкционирования, связанных с применением санкций. [19]

Деятельность в области интернет-оружия может быть в целом классифицирована как пассивная, активная или «информативная». Где в пассивном состоянии происходит бесшумный мониторинг связи; в активном, уничтожении данных и отказе в обслуживании; а в «информативном» - «. , , пропаганда, в которой используются социальные медиа и средства массовой информации для распространения информации с намерением поколебать общественное мнение ». [20]

Хорошо документированным примером интернет-вооружения, как инструмента наблюдения, является Программа PRISM. Именно здесь «Агентство национальной безопасности получило прямой доступ к системам Google, Facebook, Apple и других интернет-гигантов США». [21] Согласно экспертам Cybersecurity «Единственная самозащита от всего вышеперечисленного - универсальное шифрование. Универсальное шифрование сложно и дорого, но, к сожалению, необходимо ». [22]

В настоящее время жертвой номер один от интернет-оружия является социальный медиа, где всевозможные новости, поддельные или иные, наводняют абонентов. Социальные медиа стали «полем битвы», где в равной степени могут применяться концепции военного взаимодействия [23]. В этой напряженной информации / дезинформации войне любая слабая истина омрачена мощных ложью, которые требуют, чтобы общественность принять их, несомненно. «Исследователи все еще пытаются получить четкое представление о том, на сколько людей влияют ложные новости и их цифровое охват». [24] Последующий вопрос становится «. , , какую роль сейчас играют обычные люди в международных конфликтах? »[25]. Обыкновенные люди просто путают посторонних, которые не могут играть никакой роли.

Локализация Интернета

Для целей настоящей статьи Локализация Интернета - это концепция, в которой данные, личные или иные, находятся в суверенитете географического местоположения пользователя без внешних средств, способных блокировать доступ или изменять их без явных знаний и разрешений пользователя.

Нынешняя централизация огромных объемов деловых и персональных данных на физических серверах, расположенных в одной стране - Соединенных Штатах, представляет собой первостепенную двойную опасность. Одним из них является отсутствие плана на случай непредвиденных обстоятельств в случае потери из-за не-злокачественных причин. Другая заключается в том, что доступ к этим данным их законным владельцам зависит от политических / экономических отношений между США и страны владельцев данных.

В условиях войны любое возможное событие должно приниматься как равновероятное. Если США блокируют доступ в Интернет из страны, где ее граждане передали свои данные американским провайдерам киберслужб, полученные последствия не поддаются оценке. Частичной защитой такого возможного / вероятного враждебного действия является локализация Интернета. С сегодняшними технологическими вариантами нет смысла иметь учетную запись электронной почты, физически расположенную на расстоянии 3000 миль, особенно если она попадает в другую страну. Также нет смысла иметь электронный магазин на расстоянии 3000 миль, когда адресный рынок находится по соседству.

Учитывая, что «правительства США и Великобритании регулярно контролируют частные (интернет) коммуникации. , , ряд стран рассматривают новый тип закона, называемый «локализация данных». [26]. Такие законы обязывают предприятия, работающие в Интернете, хранить свои данные и данные своих клиентов в территориальном суверенитете страны, где происходят предприятия, вместо того, чтобы держаться на серверах, расположенных в других странах. «Вьетнам, Китай, Индонезия и Индия применяют аналогичные законы». Однако «Бразилия осуществила, но позже удалила локализацию данных, по сообщениям, из-за ее возможного экономического ущерба» [27]. Гениальному признанию не следует признать, что изъятие закона находилось под давлением международных операторов облаков.

В России закон о локализации данных требует, чтобы ". , , все персональные данные российских пользователей должны храниться в центрах обработки данных внутри границ страны. , , «Для продолжения ведения бизнеса в России многие компании, в том числе». , , eBay, Google и другие находятся в процессе или уже перенесли данные пользователя в страну. «Кроме того,». , , eBay передает данные из Швейцарии в Россию ». [27].

По мнению экономистов, применение законов о локализации данных будет стоить индустрии облачных вычислений США около 60 миллиардов долларов США в год. При локализации данных эта сумма не только станет доходом для соответствующих местных экономик, но также увеличит местные кибер-навыки и занятость. Локализация данных никоим образом не изменяет концепцию глобализации Интернета.

В заключение, проблема локализации данных в основном связана с проблемой государственной безопасности с последующими экономическими аспектами и обеспечивает частичную защиту от растущего интернет-вооружения.

связи

[1] Who owns the Internet?
Кто владеет Интернетом?
___https://www.weforum.org/agenda/2016/08/who-owns-the-internet-and-who-should-control-it

[2] Internet Corporation for Assigned Names and Numbers
Интернет-корпорация по присвоению имен и номеров
http://www.icann.org

[3] Wikipedia on ICANN
Википедия в ICANN
https://en.wikipedia.org/wiki/ICANN

[4] Internet Major Nodes Map
Карта основных узлов Интернета
https://www.internetexchangemap.com

[5] Global Commission on Internet Governance
Глобальная комиссия по управлению Интернетом
https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%206web.pdf

[6] US Department of the Treasury – Sanctions Program
Департамент США по казначейству - Программа санкций
https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

[7] Effects of the Internet on politics: Research roundup
Влияние Интернета на политику: обзор исследований
___https://journalistsresource.org/studies/politics/citizen-action/research-internet-effects-politics-key-studies

[8] The Rise and Fall of Social Media in American Politics
Рост и падение социальных медиа в американской политике
___http://techpresident.com/news/23103/rise-and-fall-social-media-american-politics-and-how-it-may-rise-again

[9] Measuring the reach of "fake news" and online disinformation in Europe
Измерение охвата «поддельных новостей» и онлайн-дезинформации в Европе
___https://reutersinstitute.politics.ox.ac.uk/our-research/measuring-reach-fake-news-and-online-disinformation-europe

[10] Living in Digital Darkness: A Handbook on Internet Shutdowns in India
Жизнь в цифровой темноте: справочник по отключению Интернета в Индии
https://sflc.in/sites/default/files/reports/Living%20in%20Digital%20Darkness%20-%20A%20Handbook%20on%20Internet_%20Shutdowns%20in%20India%2c%20May%202018%20-%20by%20SFLCin.pdf

[11] Internet Shutdowns in India
Интернет-остановки в Индии
https://internetshutdowns.in/

[12] Algeria and Iraq shut Internet to prevent exam cheating
Алжир и Ирак закрыли Интернет, чтобы предотвратить обманывание экзаменов
https://www.aljazeera.com/news/2018/06/algeria-iraq-shut-internet-prevent-exam-cheating-180621074343644.html

[13] Egypt Shuts Down Internet and Cellphone Services
Египет закрывает интернет и услуги мобильного телефона
https://www.wsj.com/articles/SB10001424052748703956604576110453371369740

[14] Russia cuts off internet in Crimea
Россия разрезает интернет в Крыму
https://www.buzzfeednews.com/article/hayesbrown/russia-cut-off-the-internet-in-crimea

[15] Who Shut Down the Internet Friday?
Кто закрыл Интернет в пятницу?
https://www.nbcnews.com/news/us-news/who-shut-down-u-s-internet-friday-n671011

[16] Stuxnet Malware
Вредоносная программа Stuxnet
https://en.wikipedia.org/wiki/Stuxnet

[17] The Love Letter Malware
Влюбленное письмо любви
https://www.symantec.com/security-center/writeup/2000-121815-2258-99?tabid=2

[18] Cyber Related Sanctions Program
Программа санкций, связанных с использованием киберата
https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf

[19] Cyber Related Sanctions Regulations
Кибер-связанные правила санкций
https://www.ecfr.gov/cgi-bin/text-idx?SID=41f7a6c1c344bde4b08d2667df8dbf1d&mc=true&node=pt31.3.578&rgn=div5

[20] The Weaponization of the Internet: Options & Tactics for States
Оружие в Интернете: варианты и тактика для государств
https://medium.com/@jessesandoval/the-weaponization-of-the-internet-options-tactics-for-states-2686df1b776c

[21] NSA PRISM Program
Программа ПРИЗМ NSA
https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[22] Our Government has Weaponized the Internet
Наше правительство вооружило Интернет
https://securityintelligence.com/the-weaponization-of-iot-rise-of-the-thingbots/

[23] Thomas Nissen: The Weaponization of Social Media
Томас Ниссен: вооружение социальных сетей
https://www.stratcomcoe.org/thomas-nissen-weaponization-social-media

[24] What research says about how bad information spreads online
В каком исследовании говорится о том, как плохая информация распространяется в Интернете
https://journalistsresource.org/studies/society/news-media/fake-news-bad-information-online-research

[25] LikeWarBook: The Weaponization of Social Media
Как военная книга: вооружение социальных сетей
https://www.likewarbook.com

[26] Will Data Localization Kill the Internet?
Будет ли локализация данных убивать Интернет?
https://www.ecommercetimes.com/story/79946.html

[27] Firms Rethink Russian Data Center Strategy, as Data Sovereignty Law Nears Activation
Фирмы пересматривают стратегию российского центра обработки данных, поскольку закон о суверенитете данных приближается к активации
https://www.datacenterknowledge.com/archives/2015/07/21/russian-data-localization-law-spurs-data-center-strategy-changes/