Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Санджай Гоэль, *Connections QJ* 19, № 1 (2020): 85-100
https://doi.org/10.11610/Connections.rus.19.1.07

Точки зрения практиков и академических кругов

Национальная стратегия кибербезопасности и появление жестких цифровых границ

Санджай Гоэль

Центр информационной криминалистики и обеспечения доступности, целостности и безопасности информации штата Нью-Йорк, Университет Олбани, 1400 Вашингтон авеню, Олбани, NY 12222, https://www.albany.edu/cifa/

Резюме: Развитию Интернета и инновациям, чье бурное развитие связано с ним, способствовала среда, которая была относительно свободна от контроля. К сожалению, однако, в результате глубокой интеграции в социальную рамку, Интернет стал потенциальным инструментом для оказания влияния на геополитические конфликты, включая вмешательство во внутренние дела других государств, подрыв национальной безопасности, дестабилизация финансовой инфраструктуры и атаки на критическую инфраструктуру. Хотя государства получают социальные и экономические выгоды от Интернета, они боятся угрозы, которую он представляет для национальной безопасности. В ответ на эти угрозы страны начинают ужесточать свои интернет границы и разрабатывают свое кибер вооружение не только как инструмент для сдерживания, но и для оказания давления во время конфликтов. Потенциальным недостатком такой регуляции, вводимой каждым отдельным государством, является замедление инновационного процесса, который Интернет традиционно стимулировал, и ограничение свободы речи, которая способствовала социальной интеграции в обществе. С другой стороны, инновации и свобода не могут процветать в хаотической среде со свирепствующей преступностью и отсутствием правил, норм и этики. Учитывая это, субъекты, формирующие национальную политику, сталкиваются с вызовом найти баланс между регуляцией и потенциальном хаосе в Интернете, и в то же время способствовать развитию свобод. В попытках найти такой баланс в национальных интересах, границы в киберпространстве играют важную роль наряду с международными усилиями по установлению

доверия в киберпространстве и замедлению фрагментации Интернета. В этой статье рассматривается вопрос о том, как эскалируют кибер конфликты, как увеличивается взаимное недоверие, и как национальные государства адаптируются к постоянно меняющемуся кибер домену.

Ключевые слова: Кибер угрозы, критическая инфраструктура, кибер конфликт, международное право.

Введение

Изощренность и результативность кибератак постоянно повышались со времени первой кибератаки червя Морриса в 1988,[1] и в последнее время стали ключевой частью стратегий национальной обороны нескольких стран. Кибер пространство сейчас считается отдельным доменом конфликта наряду с сушей, морем, воздухом и космосом, четко обозначенным в военных доктринах наиболее сильных в мире государств, т.е. России, Китая и США. Каждая страна укрепляет свою защиту, и в то же время неистово работает над разработкой кибер оружий и испытывает кибер защиту других стран. Кибератаки уже использовались для дополнения военных интервенций в ответ на политику и действия других стран и для вмешательства в выборы других стран. Свирепая гонка кибер вооружений не показывает никаких признаков ослабления. Сейчас государства сталкиваются с дилеммой: работать ли в сотрудничестве для деэскалации гонки кибер вооружений и чтобы позволить Интернету процветать беспрепятственно, или возвести границы в Интернете и подвергнуть угрозе его рост и эволюцию.

Было сделано несколько попыток выработать договор о сдерживании роста кибер вооружений; однако, отсутствие атрибуции, увеличение уязвимостей, эскалация экономического соперничества между государствами делают достижение консенсуса по этим договорам очень трудным. Хотя атрибуция при кибер инцидентах постоянно улучшается благодаря усовершенствованным аналитическим технологиям, деятельность государств в сфере разработки кибер оружий все еще находится под покровом. С точки зрения теории игр, ситуация предполагает, что каждое государство пытается максимизировать свой кибер арсенал полагая, что другие страны тоже максимизируют свои усилия по разработке кибер арсеналов. Наиболее ранние случаи использования кибер оружия имели место в конфликтах между Россией и бывшими советскими республиками Грузией и Эстонией. В этих случаях атаки были использованы для медиа пропаганды, искажения вебсайтов и т.д. С течением времени, однако, кибератаки стали более изощ-

[1] Craig Timberg, “Net of Insecurity: A Flaw in the Design,’’ *The Washington Post*, May 30, 2015, по состоянию на 13 августа 2018, https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1.

ренными, целенаправленными и опасными. Так же, большее число национальных государств обращается к кибератакам и начинает использовать кибератаки для достижения своих геополитических целей.

В статье рассмотрены текущие вызовы и обсуждаются потенциальные результаты этого конфликта. В разделе 2 представлен список ключевых инцидентов за последние 20 лет, который демонстрирует эскалацию изощренности и результативности кибератак, осуществляемых национальными государствами. В разделе 3 обсуждается как будущая эволюция Интернета экспоненциально расширяет ландшафт угроз. В разделе 4 рассматривается вопрос о том, как государства реагируют на эскалацию кибер угроз путем укрепления и начинают осуществлять режим мониторинга и цензурирования в пределах своих границ. В разделе 5 рассматриваются международные усилия по установлению доверия и развитию сотрудничества в киберпространстве для предотвращения балканизации Интернета и для замедления гонки кибер вооружений.

Эволюция средств для ведения кибервойны

Операция Аврора, инициированная Китаем в 2006, является целенаправленной кибератакой с использованием вредоносного программного обеспечения против, по крайней мере, 30 больших компаний – включая Google и Adobe, — в которой использовался недостаток нулевого дня в браузере Internet Explorer. Недостаток позволял вредоносной программе загрузиться на компьютеры пользователей. Похоже, хакеры имели доступ к исходному коду множества программных продуктов. Пятеро членов подразделения 61398 Китайской освободительной армии были «назначены» для проведения широкомасштабной кампании целевого фишинга «сперфишинг», чтобы предположительно взломать системы ведущих компаний США. Атака включала взлом компьютерных систем 141 компаний из 20 основных индустрий с 2006 по 2014 год. Хакеры искали американские коммерческие секреты: у Westinghouse, например, они взяли планы определенного типа атомной электростанции. Это первый случай, когда был использован термин «продвинутая постоянная угроза».

Stuxnet, раскрытый в 2010, был вредоносной программой типа червь, которая, как полагают, была разработана Соединенными Штатами и Израилем для воздействия на иранскую ядерную программу путем заражения программируемых логических контроллеров (ПЛК) центрифуг в иранских реакторах. Есть предположение, что эта вредоносная программа была введена через флэшки ядерных инспекторов, посланных в Иран МАГАТЭ. Эта вредоносная программа разрушала центрифуги увеличивая их скорость вращения выше допустимого рабочего предела.

Операция Дровокол, начатая из Ирана в 2012, представляла собой кампанию существенного глобального наблюдения и инфильтрации, включая ВМФ США. Она успешно избегала обнаружения и использовала обыкновенные инструменты для совершения атак и для компрометации объектов

нападения по всему свету. В число объектов воздействия входили вооруженные силы, сооружения нефте- и газодобычи, транспорт, авиалинии, аэропорты, больницы, телекоммуникации, технологии, образование, аэрокосмическая индустрия, военно-промышленная база (ВПБ), химические компании и правительства. Результатом атак стала кража чувствительной информации или захват управления сетей критической инфраструктуры во многих странах, в том числе Канаде, Китае, Англии, Франции, Германии, Индии, Израиле, Кувейте, Мехико, Пакистане, Катаре, Саудовской Аравии, Южной Корее, Турции и Объединенных Арабских Эмиратах и Соединенных Штатах.

Атака ОГУ. Атака на офис государственного управления (ОГУ) началась в марте 2014, объектом были государственные данные США, и в результате были украдены 21 миллион записей. Взлом компрометировал персональную информацию (номера социальной страховки, даты рождения, адреса и т.д.) и подробную личную информацию, связанную с выдачей разрешений на доступ к секретной информации. Атакующие получили настоящие удостоверения пользователей для систем, которые были объектами нападения, возможно, через социальный инжиниринг. Взлом состоял в загрузке пакета вредоносных программ в сеть ОГУ и создания заднего входа. Оттуда атакующие расширяли свои привилегии для получения доступа к другим системам и данным ОГУ.

Взлом НКД. Во время выборов в 2016 году в США была оркестрована из России атака на серверы электронной почты Национального комитета Демократической партии (НКД) на Gmail аккаунт руководителя кампании Хиллари Клинтон, Джона Подеста. Были украдены и впоследствии опубликованы в Wikileaks более 60 000 электронных писем, что привело к отставкам высокопоставленных официальных лиц и большому конфузу для НКД и кампании Клинтон.

NotPetya. В 2017 вредоносная программа NotPetya начала распространяться с серверов неподозревающей украинской фирмы для программного обеспечения к некоторым из самых больших бизнесов по всему свету, парализуя их операции. В число пострадавших больших корпораций входили Merck, которая потеряла 870 миллионов, Saint-Gobain, которая потеряла 384 миллионов, и Maersk, которая потеряла 300 миллионов, а общие потери исчислялись свыше 10 миллиардов долларов. Есть подозрения, что атака была инициирована по распоряжению российских военных.

Каждая из этих атак имела четкую политическую цель, например, вмешательство в выборы, оказание экономического давления во время конфликта, ответ на атаку противника и сбор военных разведданных. Последствия атак становятся все более опасными, а авантюризм стран продолжает увеличиваться. Страны прибегают к кибератакам, вместо к конвенциональным атакам из-за туманной атрибуции и меньших опасений подвергнуться международному осуждению. Ставки повышаются еще больше, поскольку

кибер-физические системы становятся все более зрелыми и получают признание в обществе, например, автономные машины, вживляемые и носимые на себе устройства и смарт измерения. Эти последствия рассматриваются в следующем разделе.

Расширение ландшафта уязвимости

Тремя главными инновациями этого десятилетия являются смарт сеть, связанные транспортные средства и вживляемые в человека устройства. Все эти три инновации радикальным образом изменят общество в разных аспектах, некоторые из которых в настоящее время трудно даже себе представить. Дискуссии, связанные с кибер-физическими системами, очень своевременны, поскольку их влияние на будущее общества будет огромным.

Мы создаем сети трех классов: монолитные сети устройств и датчиков в энергосистеме; миллионы ад хок сетей в транспортной сети; и огромная персональную сеть, состоящая из носимых устройств. В каждой из этих сетей имеется множество вызовов. Большая часть дискуссий здесь связана со статическими сетями таких кибер-физических систем, как управление промышленным производством, электроснабжение и газораспределение. Пока еще не рассматривались постоянно меняющиеся системы связанных транспортных средств и носимых устройств. Давайте рассмотрим более подробно эволюцию Интернета Вещей (ИВ).

По оценке Гартнера в следующие несколько лет в обиходе будут 21 миллиард ИВ устройств. По оценке Cisco таких устройств будет более 50 миллиардов, а Intel идет еще дальше, прогнозируя использование 200 миллиардов ИВ устройств.[2] И действительно, мы только начинаем понимать потенциал и возможности Интернета Вещей. Перечень возможных выгод расширяется по мере их поступления – повышение эффективности, оптимизация процессов и уменьшение расходов являются самыми важными, которые будут иметь место для всякого рода деловых предприятий. Первая революция началась с создания механического ткацкого станка (1784). Вторая промышленная революция началась с появления сборочной линии (1870), и третья индустриальная революция пришла с введением ПЛК (1969). Четвертая революция происходит сейчас, и движущей силой являются сенсоры, Искусственный Интеллект (ИИ) и робототехника.

Представьте себе на мгновение смарт фермерство и увеличение производительности и точности прогнозов, которые можно будет осуществить, когда датчики смогут давать точно настроенную информацию о темпера-

[2] Nathan Eddy, “Gartner: 21 Billion IoT Devices to Invade By 2020,” *Information Week*, October 11, 2015, по состоянию на 11 апреля 2018, www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081.

туре и влажности, pH почвы и содержания питательных веществ для информирования сельских хозяйств и увеличения урожайности. Или замечательный потенциал в медицине и биомедицинской информатике инсулиновых насосов, которые могут осуществлять мониторинг уровня сахара в крови и настраивать уровень инсулина в *реальном времени*, или систему Медицинское сито IBM, которая с помощью интеллигентных алгоритмов и передового ИИ производит сортировку всей медицинской истории пациента в поиске подсказок для составления анализа изображений; узнавать все, что нужно знать о пациенте в течение секунд для составления более интеллигентного диагноза и бесконечно более персонализированного плана лечения.[3]

Представьте себе возможность использовать время, которое сейчас вы тратите на борьбу с транспортом при своих ежедневных поездках, на чтение или даже на мечтательные размышления в своем автономном транспортном средстве. Университет Олбани работает над проектом, при котором дорожные указатели могут коммуникировать друг с другом, подстраиваясь так, чтобы увеличивать транспортный поток. Представьте себе систему сенсоров, которые могут предсказывать землетрясения *до* того, как они произойдут; и улучшения, которые можно осуществить в результате более широкого мониторинга в реальном времени потребления энергии и экологических параметров. ИВ трансформировал мир производства и трансформации электрической энергии. Сегодня мы создаем архитектуру энергосистемы, которая будет интегрировать множество отдельных энергосистем и сделает ее более устойчивой. Наложением коммуникационной сети на энергосистему и созданием информационной системы, которая сможет связать датчики через электросеть, чтобы сделать ее более устойчивой, будет создан интегрированный рынок электрической энергии, на котором каждый сможет покупать и продавать электричество.

Сейчас 54 % людей в мире живет в городах, а к 2050 ожидается, что их доля дойдет до 66 %. В сочетании с общим увеличением численности населения, урбанизация добавит в течение следующих тридцати лет еще 2.5 миллиардов людей к населению городов. Быстрая урбанизация создает большое экологическое напряжение. Экологическая, социальная и экономическая устойчивость должны развиваться одновременно с быстрым расширением, что еще больше нагружает ресурсы наших городов. Целью смарт городов является содействие устойчивому развитию для разрешения проблем урбанизации. Эффективное использование данных инфраструктуры и данных о собственных потребностях городских сообществ может улучшить

[3] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in *Proceedings of 2012 10th International Conference on Frontiers of Information Technology (FIT)* (Institute of Electrical and Electronics Engineers, December 2012), 257-260, https://doi.org/10.1109/FIT.2012.53.

распределение энергии, оптимизировать сбор мусора, уменьшить дорожные заторы и даже улучшить качество воздуха с помощью ИВ.

Как мы можем защитить себя от взломов, кибератак и кражи данных? В городах, где множество участников обмениваются информацией, как мы можем быть уверены, что участник являются тем, что он о себе говорит? И как мы можем знать, что данные, которыми они делятся, являются верными и точными? Наряду с безграничными перспективами приходит и огромный риск в смысле ущерба безопасности и конфиденциальности, взлома и нарушения работы систем. Когда критическая инфраструктура – электростанции, водоснабжение, аэропорты и больницы – управляются ИВ системами, потенциальная опасность человеческих потерь – от сбоев до киберуголовной деятельности – нарастает экспоненциально.[4]

Риски ИВ не домыслы, они уже здесь. Согласно исследованию фирмы Hewlett Packard, 80 % проверенных ИВ устройств (они проверяли широко используемые домашние системы сигнализации и термостаты, автоматические замки для гаражных дверей и т.д.) вызывали опасения в смысле конфиденциальности в среднем с 25 % пробелов безопасности для отдельного устройства.[5] В 2016 была инициирована DDoS атака — самая большая в истории — на сервис провайдере с использованием ИВ бота с вредоносной программой, называемой Mirai, что привело к выключению больших частей Интернета — в том числе Twitter, Netflix, Reddit. После проникновения Mirai в систему она заставляет компьютеры постоянно искать в Интернете уязвимые ИВ устройства и, используя имена потребителей и пароли по подразумеванию, производить регистрацию, заражая их тоже программой Mirai.

Безопасность нашего будущего – еры ИВ – будет настолько надежна, насколько надежна безопасность каждого из миллиардов маленьких связанных устройств, которые компрометируют наши системы. У нас у всех случалось, что компьютер отказывал и мы теряли документ или таблицу, но представьте себе, что откажут кардиостимулятор или дигитализированный инсулиновый насос, которые могут быть взломаны, что приведет к смерти человека, или Volkswagen, взламывающие компьютерную систему своих собственных машин для обхождения ограничений экологического контроля. Представьте себе, как хакеры получают доступ к банковским данным и опустошают счета. Неавторизированный персонал может получить доступ к смарт устройствам, в которых хранится чувствительная информация о финансовых счетах, пароли или другая информация, используя уязвимости

---

[4] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu, "Handling a Trillion (Unfixable) Flaws on a Billion Devices: Rethinking Network Security for the Internet-of-Things," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks* (ACM, November 2015), http://dx.doi.org/10.1145/2834050.2834095.

[5] "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," *HP News*, July 29, 2014, https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676.

для кражи идентичности или для совершения мошенничеств. В докладе Федеральной торговой комиссии США приводится оценка, что 10 000 домашних хозяйств могут генерировать ежедневно до 150 миллионов записей данных, предоставляя значительное число точек входа для хакеров.[6]

Национальные государства знают об этих уязвимостях и будут пытаться использовать их против других стран для утверждения своего суверенитета в Интернете. Концепция цифровых границ и Интернет суверенитета превратилась от концепции в действительность, и несколько стран уже работают над контролем информационных потоков через их границы, а также и над активным мониторингом и цензурированием информации в рамках своих границ, что мы рассмотрим в следующем пункте.

Балканизация Интернета

Интернет работал со свободным доступом и с международным суверенитетом в течение многих лет, что позволяло ему расти и превращаться во всеобщую коммуникационную платформу, которая сейчас играет роль социального клея для общества, и в платформу для коммерции и торговли. Один из доводов против ограничений Интернета то, что информация является международным человеческим правом. Более практическим и экономически сильным аргументом является то, что международная торговля зависит от доступа к Интернету и трансграничного потока данных. Открытый и свободный доступ к Интернету есть то, что делает Интернет очень успешным – но этот доступ также стал и самым большим вызовом.

Огромное влияние Интернета на общественное мнение и на развитие торговли делают его объектом милитаризации. Как заметил министр обороны США Панетта, «Интернет открыт. Он легко доступен, как и должно быть. Но это превращает его в новую сферу военных действий. Это поле боя будущего».[7] Он используется для воздействия на общественное мнение и для оказания поддержке смене режима, для совершения атак на информационную инфраструктуру национальных государств, для вербовки новых членов террористических организаций и для того, чтобы ставить под угрозу и нарушать работу критической инфраструктуры. Для киберпространства уникально (по сравнению с другими физическими средами, как земля, воздух и космос) то, что хотя оно глобально, но цена входа в него очень низкая.

Пропаганда и инакомыслие давно являются активными силами в странах, но сам масштаб и охват Интернета сделал его могучим оружием. Будь

---

[6] Federal Trade Commission, “Internet of Things: Privacy and Security in a Connected World,” FTC Staff Report (January 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[7] Joshua P. Meltzer, “The Internet, Cross-Border Data Flows and International Trade,” *SSRN Electronic Journal*, April 1, 2013, http://dx.doi.org/10.2139/ssrn.2292477.

то видеоролики протестов или полицейской жестокости в YouTube, или новые эффективные инструменты Интернет агитации, Интернет играет важную роль в политической организации. Акторы – даже индивидуальные акторы – могут оказывать могучее влияние в киберпространстве, которое на порядки сильнее, чем могут осуществить небольшая группа государств, которые действуют в сухопутном, воздушном, морском и космическом оперативных доменах.

Интернет является доменом, который для всех остальных оперативных доменов играет роль необходимого (если не абсолютно необходимого) фактора. Учитывая огромную мощь Интернета, и в ответ на его использование в политических и военных целях, концепция международного суверенитета Интернета быстро сдвигается в сторону концепции суверенных Интернет границ. Эта трансформация ускоряется в результате ужесточения границ Интернета в последние годы. Государства от Китая до Ирана и Бирмы во все большей степени фильтруют и блокируют доступ к медиа и блогам, которые пропагандируют политические взгляды, противоречащие правительственным.

Изначальной и по существу либертарианской природе Интернета все чаще бросают вызов претензии государств на юрисдикцию над Интернетом или разработка правил, которые ограничивают возможность людей и компаний иметь доступ к Интернету и перемещать данные через государственные границы. Наличные инструменты для ограничения доступа к Интернету и трансграничного потока данных становятся все более доступными, сложными и широко адаптируемыми. В их число входят блокирование основного протокола или точек доступа в стране и фильтрование имен доменов, интернет протоколов или URL. Государства могут ограничивать доступ к Интернету и непрямыми способами, которые ограничивают работу поисковиков, например ставя условия в лицензии на работу или не посылая конкретные материалы и накладывая жесткие наказания за несоблюдение ограничений. Контроль над информацией – для стран, которые пошли по этому пути – включает ограничение доступа к иностранным информационным источникам, блокировку таких иностранных интернет инструментов, как Google search, Facebook, Twitter и определенные мобильные приложения, и предъявления требования иностранным компаниям адаптироваться к внутригосударственным регуляциям.[8] Однако, включая все большее количество инструментов контроля, мы душим Интернет и он работает все медленнее. Легитимность создания национальных границ в Интернете государствами проистекает из правил, предположительно предназначенных для защиты граждан от пагубного внешнего влияния.

Давайте рассмотрим увеличивающуюся балканизацию Интернета, поскольку некоторые страны работают на установление национальных гра-

[8] Meltzer, “The Internet, Cross-Border Data Flows.”

ниц, тогда как другие борются за изначальный, предполагающий свободный доступ интернационализм Интернета. Затем мы более подробно рассмотрим эту дихотомию в контексте растущей милитаризации Интернета и ускоренного развития средств кибер войны. Фальшивая ли это дилемма, когда некие государства – как например, Соединенные Штаты – пропагандируют Интернет без границ, а сами разрабатывают средства кибер войны и кибер обороны? Давайте сперва рассмотрим картину Интернет границ – кто что делает по этому вопросу.

Ужесточение Интернет границ для обеспечения национальной безопасности

Появление Интернета в Китае трансформировало китайские СМИ от замкнутой и централизованной системы в открытую и децентрализованную систему. В Китае новое поколение активно включается в Интернет.[9] К концу 2017 в Китае было 722 миллиона интернет потребителей, что составляет 55.8%, и это самое большое онлайн население в мире. Китай существенно расширил технологический потенциал и человеческий капитал, направленный на контролирование интернет содержания, включая принятия на работу, по некоторым оценкам, от 500 000 до 2 000 000 Интернет пропагандистов (более известная как 50-центовая армия), которые пишут интернет комментарии в защиту престижа и целостности Китайской коммунистической партии.[10]

Китай, Саудовская Аравия, Иран и другие имеют похожие амбиции в отношении Интернета: они думают, что государству следует решать какая информация пересекает его границы, а не компаниям и НПО. В докладе 2018 года Freedom House исследовалось состояние в 65 странах и было установлено, что с предыдущего года Интернет свобода уменьшилась в 26 из них, причем половина этого уменьшения была связана с выборами.[11]

Китай, как архитектор «кибер-суверенности», начал экспортировать свой режим цензурирования Интернета в другие страны, изменяя Интернет снизу вверх. Согласно докладу Freedom House, как минимум 36 государств, включая Египет, Саудовскую Аравию и Вьетнам, получили осуществленную при закрытых дверях подготовку по «новому медиа и информационному менеджменту». Последние несколько лет Китай принимал представителей СМИ дюжины государств для проведения двух- и трехнедельных семинаров

---

[9] Wenfang Tang and Shanto Iyengar, eds., *Political Communication in China: Convergence or Divergence Between the Media and Political System?* (London: Routledge, 2012).

[10] Tenzin Dalha, “Assertion of China’s Sovereignty over the Internet,” *global-is-asian*, October 4, 2018, https://lkyspp.nus.edu.sg/gia/article/assertion-of-china's-sovereignty-over-the-internet.

[11] Adrian Shahbaz, “Freedom on the Net 2018: The Rise of Digital Authoritarianism,” Freedom House, 2018, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

для ознакомления с его системой мониторинга и цензуры и поставлял телекоммуникационное оборудование, передовую технологию распознавания лиц и инструменты для анализа данных разным государствам с проблемами в области прав человека. Имеются свидетельства, что некоторые страны, например Уганда, используют китайское программное обеспечение для мониторинга местного Интернета под предлогом борьбы с преступностью.

Учитывая широкий спектр глобальных инцидентов, как NotPetya, вмешательство в выборы и опасные ситуации, которые могут вызвать такие инциденты, многие страны воспринимают более авторитарный подход к Интернету. В ноябре 2018 резолюция по киберпреступности, поддерживаемая Россией, и принятая Генеральной ассамблеей ООН, была поддержана тремя наибольшими демократическими государствами в мире – Индией, Бразилией и Нигерией, которые проголосовали вместе с Россией и Китаем, разойдясь во мнении с такими традиционно более открытыми странами, как Австралия, Канада, Эстония, Франция, Греция, Израиль, Соединенные Штаты и Объединенное Королевство. В конце 2018 и начале 2019 были приняты законы, которые ограничивали интернет свободы во имя снижения уязвимости и для борьбы с киберпреступностью во Вьетнаме, Таиланде, Египте, Объединенных Арабских Эмиратах и Танзании.[12]

Правительство России усиливает контроль над Интернетом, и Россия не одинока в этом. В ходе подготовки выборов в 2018, когда Путин был избран на второй срок, власти усилили свою уже и без того жесткую хватку над Интернетом, блокируя Telegram, популярный мессенджер с более 10 миллионами русских пользователей, так как эта платформа отказалась передать ключи криптирования ФСБ. Имели место протесты против законодательных попыток изолировать российский Интернет, сделав его автономным под предлогом защиты от внешних «угроз». Критики предупреждают, что закон о так называемом «суверенном» Интернете будет действовать в качестве некоего рода «железного занавеса» и будет служить инструментом правительства для наложения цензуры на проявления инакомыслия в социальных медиа. Имеется информация, что паранойя в китайском и российском стиле по поводу неограниченного онлайн дискурса начинает вызывать резонанс на Западе. Киерон О'Хара, профессор по компьютерным наукам и эксперт по управлению Интернета, считает, что западные демократии начинают сходиться с Китаем и Россией в общих страхах, что приводит к общему аффинитету к некоей модели «авторитарного Интернета».[13]

---

[12] Justin Sherman, "How to Regulate the Internet Without Becoming a Dictator," *Foreign Policy*, February 18, 2019, https://foreignpolicy.com/2019/02/18/how-to-regulate-the-internet-without-becoming-a-dictator-uk-britain-cybersecurity-china-russia-data-content-filtering.

[13] Eduard Saakashvili, "The Global Rise of Internet Sovereignty," *.coda*, March 21, 2019, https://codastory.com/authoritarian-tech/global-rise-internet-sovereignty/.

Такое ужесточение не является чисто восточным явлением – после вмешательства в президентские выборы США имели место большие дебаты о том, как контролировать пропаганду в социальных медиа – что является формой цензуры. Интернет медиа компании, Facebook и Google, просят играть ведущую роль в искоренении фальшивых новостей на их вебсайтах. Кое-кто может и не находить большой разницы, но тогда, когда США пытаются искоренить фальшивую информацию, другие страны пытаются искоренить настоящие дебаты между своими гражданами.

Экономики и общества по всему миру тесно переплетены Интернетом через весь спектр социума, включая коммерцию, коммуникации, образование и социальные отношения. Государства должны получить передышку от эскалации кибератак, вмешательства во внутреннюю политику и потенциальных человеческих и имущественных потерь. Было предпринято несколько попыток сдержать кибервойну путем принятия кибер договоров и норм, что является предметом следующего параграфа.

Дипломатические сдержки для де-эскалации гонки кибер вооружений

Нормы и кодекс поведения в киберпространстве являются предметом множества дискуссий. В идеале, нормы должны быть направлены на обеспечение свободного потока информации в Интернете на пользу людям. Однако, дискуссии сместились в сторону того, кто, что и когда может считаться нападением в Интернете, и каковы могут быть последствия таких атак.

Три ГПЭ (Группы правительственных экспертов) в ООН еще до 2016/2017 инициировали и продвигают вперед международный диалог о кибербезопасности с 2010 года, в основном по нормам и мерам установления доверия в киберпространстве. Группе 2016/2017 была поставлена задача определить, «как международное право применяется к использованию информационных и коммуникационных технологий государствами». Этот вопрос – международное право и его применение – является критически важным пунктом.

В 2017 году было опубликовано «Таллиннское руководство 2.0 по международному праву, применимому к кибер операциям», авторами которого были девятнадцать экспертов по международному праву. Это руководство актуализировало анализ от 2013 года как существующее международное право применяется к киберпространству. Примечательно то, что новое издание всего через четыре года включало изменение названия книги, упоминающее не «кибер войну», а «кибер операции»; отражение того факта, что сегодня кибератаки обычно попадают в категорию ниже порога, при котором международное право объявляло бы их формальным актом войны.[14]

[14] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

В последние годы ОБСЕ также работает над развитием мер по укреплению доверия (МУД) и достигла определенного успеха в достижении консенсуса по предварительным пунктам. Основной целью таких МУД является повышение прозрачности между государствами путем поощрения обмена информацией и коммуникациями между субъектами, определяющими политику и принимающими решения. Есть надежда, что хотя такие МУД не смогут остановить преднамеренный конфликт, они, возможно, смогут смягчить последствия непреднамеренных действий, замедляя эскалацию событий.

Нормы США об операциях в воздухе, на суше и на море в принципе проистекают из Вестфальской концепции суверенитета: «в своих международных отношениях все члены должны воздерживаться от использования силы против территориальной целостности или политической независимости любого государства»,[15] т.е. ответственное поведение должно подразумевать определенную схему оперативного сдерживания.

Без соглашения о международном праве и его применении к кибер домену, включая верификацию и атрибуцию инцидентов, многие другие аспекты (включая нормы, меры по укреплению доверия и создание потенциала) остаются неопределенными, поскольку похоже, что точки зрения расходятся и позиции становятся более жесткими, а не наоборот. Одним из основных вопросов по кибер домену является вопрос, следуют ли кибер операции – в которых участвует большинство, если не все страны – схеме оперативного сдерживания или схеме эскалации.

Являются ли кибератаки ответными или стратегическими наступательными действиями национальных государств

Являются ли кибер операции изначально сдерживающими? Предназначены ли они для эскалации или нет? Эффективны ли они в качестве инструментов и маневров внешней политики? Кое-кто может возражать, что характеристики операции в киберпространстве – включая неопределенность результатов и реакций и центральную проблему отсутствия атрибуции и верификации – похоже, по своему характеру, являются эскалирующими. Но так ли это? Одним из способов проводить информированную внешнюю политику, это лучшее понимание и количественная оценка текущей реальности. Недавний доклад института Като, анализирующий политику, рассматривает 272 документированных обменов кибер действий между соперничающими государствами в периоде с 2000 по 2016. При категоризации этих кибер обменов они оценили 32 % как нарушения работы, 54 % как шпионаж и 12 % как разрушение, или наиболее опасный вид атак, направленный на приведение в негодность или нанесение фундаментального ущерба объектам воздействия. Что наиболее важно, авторы исследования пришли к заключению, что большинство (68 %) не документируют схему ответных действий, т.е. большинство кибер операций не вызывают кибератак, но и не

[15] Charter of the United Nations, effective 24 October 1945, Article 2(4).

сдерживают кибератак. Они утверждают, что определенный уровень кибер операций является нормой, и что хотя киберпространство до сегодняшнего дня было доменом политической войны и принуждающей дипломатии, кибер операции не были эскалационными или особенно эффективными в достижении решительных результатов.[16] «Инциденты» или «атаки», независимо от их числа, не составляют войны – кибер войны или другой – в настоящем политическом, правовом, оперативном или фактическом смысле.[17] Тогда как многие говорят о грядущем «Кибер Перл Харборе», авторы предполагают, что домен в реальности усеян тайными операциями, направленными на управление эскалации и сдерживание будущих атак. Они рекомендуют занимать оборонительную позицию, включающую ограниченные кибер операции, направленные на сдерживание соперников и предотвращение эскалации вместо тех прокламированных администрацией Трампа изменений политики и стратегии, которые предполагают, что наступление есть эффективный и легкий способ для того, чтобы остановить попытки соперничающих государств взламывать системы Америки (позиция, которую авторы называют опасным мифом).

Кое-кто утверждает, что кибер операции дают эффективные средства для рассеяния и де-эскалации и предпочтительнее, чем упорные действия и упреждающие удары, Америке нужно использовать кибер операции, чтобы сеять постоянные заблуждения противника и проводить активную оборону.

Международная политика как инструмент кибер отношений

Центральным элементом позиции президента Обама было кибер сдерживание и работа над международными нормами поведения. Его Международная стратегия по киберпространству от 2011 основывалась на трех основных принципах: 1) гарантирование фундаментальных свобод (например, свобода выражения); 2) конфиденциальность и 3) свободный поток информации. В 2015 Обама добился сделки с китайцами, чтобы ограничить кибератаки, с последующим уменьшением и их числа. Президент Трамп занял другую позицию, спровоцировав рост китайско-американской напряженности своей торговой политикой и позицией Кибер командования США,[18] которое призывало к «упорным действиям для сохранения кибер

[16] Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford Scholarship Online, May 2018), https://doi.org/10.1093/oso/9780190618094.001.0001.

[17] Mika Kerttunen and Eneken Tikk, “Strategically Normative. Norms and Principles in National Cybersecurity Strategies,” *EU Cyber Direct*, April 13, 2019, https://eucyberdirect.eu/content_research/a-normative-analysis-of-national-cybersecurity-strategies/.

[18] United States Cyber Command, “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,” June 14, 2018, www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

превосходства». Это позиция активного участия и защиты от внешних сетей. Может ли такая агрессивная позиция и политика, разрешающие упреждающие наступательные киберстратегии, привести к риску пересечь порог и изменить правила игры?

В мае 2019 Генеральный секретарь НАТО сказал России и другим потенциальным противникам, что западный военный альянс готов использовать любые и все возможные средства, находящиеся в его распоряжении, в ответ на кибератаки. «Для того, чтобы сдерживание имело полную эффективность, потенциальные нападающие должны знать, что мы не ограничимся ответом в киберпространстве, когда на нас совершат нападение в киберпространстве», сказал Столтенберг во время пресс-конференции в Лондоне с министром иностранных дел Объединенного Королевства, Джереми Хантом. «Мы можем, и мы будем использовать весь набор способностей, находящихся в нашем распоряжении».[19] Может ли такая агрессивная позиция и политика, разрешающие упреждающие наступательные киберстратегии, привести к риску пересечь порог и изменить правила игры?

Выводы

За последние десять лет появилось некоторое число кибер угроз, связанных с национальными государствами, которые вызывают у государств чувство беспокойства, включая наблюдение/атаки на критическую инфраструктуру, вмешательство во внутренние дела других стран через основанной на Интернете/социальных медиа пропаганде, финансовые мошенничества, кража интеллектуальной собственности и компрометация национальной безопасности. В ответ на эти угрозы страны ужесточают свои Интернет границы. Если страны не будут чувствовать себя уверенно, ужесточение Интернет границ продолжится и быстро распространится, и пока Интернет не будет полностью демилитаризован, страны не будут чувствовать себя в безопасности. При отсутствии эффективных и верифицируемых норм, нам следует ожидать продолжения ужесточения Интернет границ и расширение мониторинга Интернета и социальных медиа. Страны продолжат создавать свои кибер арсеналы в качестве инструментов сдерживания против других государств; это будет включать дезинформационные кампании, дестабилизирующие атаки, зондирование кибер защиты и сбор разведывательной информации. Без доверия и взаимного сотрудничества будет сложно достигнуть консенсуса по нормам, и эта тенденция будет продолжаться и может привести к возможной полной фрагментации Интернета; возможно, в виде классического разделения Восток-Запад, что крайне нежелательно.

[19] "NATO Warns Russia of 'Full Range' of Responses to Cyberattack," *Security Week*, May 23, 2019, https://www.securityweek.com/nato-warns-russia-full-range-responses-cyberattack.

Во-первых, если мы позволим этой тенденции и дальше беспрепятственно развиваться, мы отступим от достижений, которые мы уже реализовали и ограничим возможность продолжать получать большие выгоды от нашей связанности в смысле лучшее здравоохранение, образование, экономическая стабильность и лучшее качество жизни. Нам нужно найти баланс, который позволит иметь свободный поток информации, и в то же время защитить чувствительную информацию на основе общественных и политических ожиданий и потребностей безопасности каждой страны. Во-вторых, нам нужно избегать в наибольшей возможной степени катастрофические последствия злонамеренного использования Интернета – нанесение ущерба здоровью и энергетической инфраструктуре, распространение эксплуатации детей и трафика женщин и рисков для национальной безопасности. Это означает проведение красных линий, вокруг которых смогут сплотится все. В-третьих, нам нужно гарантировать, что кибер война не приведет непреднамеренно к кинетическим военным действиям (включая ядерные) в результате неправильной оценки или атрибуции атак. И наконец, когда мы формируем политику, мы должны иметь в виду важность Интернета для общества и понимать риски для социальных польз от него, если мы не сумеем добиться глобального консенсуса по средствам кибер войны и не ограничим распространение кибер оружий.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторе

Санджай Гоэль является доцентом на кафедре менеджмента информационных технологий (Школа бизнеса) Университета Олбани, SUNY и директором по исследованиям Центра информационной криминалистики и доступа, целостности и безопасности информации штата Нью-Йорк при университете. Доктор Гоэль получил докторскую степень по машиностроению в 1999 в Политехническом институте Ренсселера. В сферу его нынешних научных интересов входят информационная безопасность и поведение, обеспечивающее конфиденциальность, инновационное образование и инновационную педагогику, модели безопасности, т.е. биологические модели, модели рисков, политика безопасности и кибервойна. Он ведет исследования по криминалистике и киберпреступности, критической инфраструктуре, включая конфиденциальность при анализе данных интеллигентных электросетей; влиянию безопасности и терроризма на финансовые рынки; надежной транспортировке и устойчивым сервисно-ориентированным архитектурам. *E-mail*: goel@albany.edu.

Признательность

Том 19 журнала *Connections: The Quarterly Journal* публикуется при поддержке правительства Соединенных Штатов Америки.