США и Китай: в преддверии большой войны в киберпространстве?

Евгений Прейгерман

Опубликовано на Caliber.az

Резюме

Нарастающее противостояние в киберпространстве между Вашингтоном и Пекином в политическом смысле начинает напоминать противостояние в ядерной сфере в годы Холодной войны. В зависимости от будущих решений администрации Трампа процесс может привести либо к резкой и очень опасной эскалации, либо, наоборот, к снижению напряженности и активной дипломатии.

В начале декабря в медийном пространстве США появились сообщения о том, что минимум восемь основных американских телекоммуникационных сетей подверглись кибератаке. Она была названа беспрецедентной по своим масштабам и глубине проникновения. Новость произвела эффект разорвавшейся бомбы. Правда, на фоне приближающихся рождественских праздников и в преддверии передачи ключей от Белого дома новой администрации Дональда Трампа информационная бомба получилась замедленного действия. Пока политики и комментаторы лишь громогласно констатируют шок и призывают к ошеломляющим ответным действиям. Но конкретных решений в этом направлении, судя по всему, еще нет.

Если такие действия в итоге будут предприняты, то в новом году мир впервые может столкнуться с грандиозной эскалацией напряженности в киберпространстве. Прогнозировать развитие событий при таком сценарии сложно, так как на практике открытых «боевых действий» в онлайн режиме между крупнейшими державами еще никогда не было.

> Поэтому такие события могут привести как к катастрофическому росту напряженности до уровня полноценной войны, так и, наоборот, стать триггером разрядки уже существующей геополитической наэлектризованности.

Самая масштабная кибератака в истории?

Американские СМИ ссылаются на спецслужбы, которые утверждают, что за массированной кибератакой стоит китайская хакерская группа Salt Typhoon (название придумано самими американцами). По публикуемой информации, представители группы смогли получить доступ к закрытым базам данных, как минимум, восьми крупнейших телекоммуникационных компаний. Список пострадавших включает T-Mobile, Verizon, Lumen и AT&T. Оценочно были скомпрометированы метаданные – то есть информация о звонках и сообщениях, а не о их содержании – более 1 млн человек. Самое интересное, что среди тех, в чьи телефоны, возможно, смогли проникнуть хакеры, многочисленные высокопоставленные политики и чиновники, в том числе новоизбранный президент Дональд Трамп и его вице-президент Джей Ди Вэнс.

Согласно медийным сообщениям, масштабы произошедшего таковы, что председатель Комитета по разведке Сената США Марк Уорнер назвал это «худшим телекоммуникационным взломом в нашей истории». А вероятный будущий государственный секретарь сенатор Марко Рубио заявил, что произошедшее является «самым тревожным и широкомасштабным вторжением в телекоммуникационные системы в истории мира, а не только нашей страны». С похожими оценками выступили и представители разведсообществ Австралии, Канады и Новой Зеландии.

Притом полностью прекратить забор данных до сих пор не удалось, несмотря на то, что факт произошедшего якобы стал известен американским спецслужбам еще в сентябре. Вероятно, это связано и с технической сложностью задачи, и с осторожностью американских IT-специалистов. Последние своими контрдействиями хотят минимизировать риски еще большего урона телекоммуникационной сфере страны и одновременно собрать как можно больше информации об используемых хакерами методах.

Примечательно, что это уже не первый раз за последние годы, когда Вашингтон обвиняет китайские хакерские группы в кибератаках против критической инфраструктуры США. И обвинения обычно сопровождаются медийным акцентом на том, что эти группы так или иначе аффилированы с правительством (подобные

формулировки часто используются и в отношении других неправительственных акторов, например, из России). Так, в мае 2023 года компания Microsoft заявила о китайской атаке на объекты водной и транспортной инфраструктуры на всей территории США. А в сентябре этого года директор ФБР обвинил «действовавшие по указанию правительства Китая» группы в захвате контроля над сотнями тысяч подключенных к интернету устройств, таких как видеокамеры и оборудование для хранения данных.

Китайская сторона отвергает какую-либо причастность к произошедшему. Пресс-секретарь посольства КНР в Вашингтоне назвал звучащие обвинения в адрес его страны «иррациональными» и подчеркнул, что Китай сам систематически становится объектом кибератак.

> Тем не менее в США, по крайней мере в публичном пространстве, нет другого мнения: все уверены, что внедрение в информационные системы телекоммуникационных компаний было осуществлено руками Salt Typhoon и что целью было собрать чувствительную разведывательную информацию в интересах официального Пекина.

На этом фоне в адрес действующей администрации Джозефа Байдена и будущей администрации Трампа звучат воинственные призывы ответить так, чтобы мало не показалось. К примеру, председатель Комитета по внутренней безопасности Палаты представителей республиканец Марк Грин требует от исполнительной ветви власти «начать наступление» против Китая в киберпространстве, а не ограничиваться оборонительными действиями с целью лишь защитить собственную инфраструктуру. По его словам, Вашингтон должен дать понять всему миру, что ему есть чем ответить, и «приставить нож к горлу» Китая. С похожими заявлениями выступают и многие другие политики, журналисты и эксперты.

Последует ли Белый дом их призывам, покажет уже ближайшее время. Еще месяц управлять США будет демократическая администрация, поэтому не исключено, что какие-то активные действия может предпринять именно она. Традиционно уходящее правительство в последние месяцы своей каденции воздерживается от решений, которые могут иметь долгосрочные последствия. Однако это явно не относится к администрации Байдена. Как видно на примерах кризисов на Ближнем Востоке и войны в Украине, она, наоборот, демонстрирует повышенную активность в свои финальные недели, рассчитывая добиться хоть каких-то пиар-успехов и одновременно ограничить свободу будущего маневра Трампа.

Правда, пока действующая администрация воздерживается и от обширных комментариев, и от конкретных решений в отношении хакерской группы Salt Typhoon и всей связанной с ней ситуации. Поэтому, скорее всего, этот файл она просто передаст сменщикам. Республиканскому правительству в любом случае придется уделять кибербезопасности в целом и противостоянию в этой сфере с Китаем повышенное внимание.

Во-первых, с учетом глубокого проникновения онлайн-технологий в различные уголки жизни тема киберпространства объективно имеет все более существенное значение для национальной безопасности любого государства. И уж тем более для США (равно как и Китая), претендующих на лидерские позиции во всем, в том числе информационных технологиях. Во-вторых, нарастающий общественно-политический резонанс от дела Salt Typhoon и предшествовавших кейсов кибератак, в которых американские СМИ обвинили Пекин, будет требовать от администрации Трампа решительных шагов.

> Поэтому вероятность резких и масштабных ответных действий со стороны Вашингтона уже в ближайшие месяцы действительно высока. А это, в свою очередь, сопряжено с риском серьезной эскалации.

Притом такая эскалация очень быстро может перерасти в невиданную еще в истории войну в киберпространстве между крупнейшими мировыми державами. При некоторых гипотетических сценариях подобное противостояние может и вовсе выйти за онлайн-пределы и спровоцировать кинетические столкновения даже в реальном мире.

Киберпространство как новое ядерное оружие

Подчеркнем, что пока такие наиболее катастрофические сценарии выглядят малореалистичными. Однако это не делает их менее опасными, что важно осознавать всем, кто требует «наступать, а не только защищаться».

Даже по приведенной выше цитате американского конгрессмена-республиканца Марка Грина хорошо видно, что растущее противоборство в киберпространстве повсеместно воспринимается сквозь ту же призму, что и классическое противостояние в военной сфере. Логика оппонирующих сторон здесь такая же. В частности, так же работает расчет на сдерживание оппонента: нужно показать

наши превосходящие возможности и непоколебимые волю и решительность их задействовать для защиты наших интересов. И ровно так же всегда рассуждают оппоненты.

В итоге, как и в чисто военной сфере, нацеленность противостоящих стран на обоюдное силовое сдерживание приводит к раскручиванию так называемой спирали безопасности (или «дилеммы безопасности»). То есть каждая сторона исходит из того, что повышает собственные силовые возможности и постоянно демонстрирует готовность их в полной мере задействовать исключительно для защиты и обеспечения своей безопасности. Но в глазах противоположной стороны это выглядит не иначе как угрожающая активность, которая может создать материальные и политические предпосылки для агрессии со стороны противника. Поэтому уже эта, вторая, сторона продолжает наращивать свои силы и средства и постоянно ищет слабые места в системах противника.

Такое противостояние быстро превращается в спиралевидный процесс. На каждом новом его витке повышается градус напряженности, а вместе с ним – и вероятность реального столкновения. В психологическом плане с каждым новым витком участникам все сложнее видеть в оппонирующей стороне кого-то, кроме непримиримого противника, который хочет лишь вашего полного уничтожения. А если так – то какие же могут быть переговоры?

Разорвать такой порочный круг спиралевидной эскалации можно либо незаурядным дипломатическим усилием с двух сторон, либо в результате масштабного кризиса, который приводит обоих оппонентов к осознанию неизбежных собственных потерь недопустимого масштаба в случае дальнейшего раскручивания спирали. Вернее, только оба эти фактора вместе могут сыграть стабилизирующую роль: вначале кризис приводит политиков к осознанию близкой катастрофы, после чего политики дают мандат дипломатам полноценно делать их работу.

> В середине прошлого века эти факторы сошлись воедино после появления у США и СССР способных уничтожить друг друга и всю человеческую цивилизацию ядерных арсеналов. С некоторой долей условности можно предположить, что в XXI веке подобную роль может сыграть кибероружие.

Понятно, что прямое сравнение разрушительных потенциалов этих технологий кажется некорректным. Однако с политической точки зрения они все же сопоставимы.

Как и ядерное оружие в середине XX века, киберсреда сегодня технологически очень развита, но политически плохо осознана. Как и тогда в ядерной сфере, сейчас отсутствует полноценный каркас международных договоренностей, регулирующих в достаточной степени взаимодействие и конкуренцию в киберпространстве. При этом уязвимость и государств, и конкретных людей в случае выхода ситуации в киберсфере из-под контроля, очевидно, очень высока.

Поэтому при всех рисках того, что уже в ближайшие месяцы мир столкнется с реальностью большой кибервойны, есть также возможности использовать сложившуюся ситуацию как почву для начала конструктивного переговорного процесса. Для деконфликтинга и налаживания профессиональных и политических каналов, которые помогут в выстраивании общего доверия как между Вашингтоном и Пекином, так и в многостороннем формате, что особенно важно с учетом выкристаллизовывающейся многополярности. И то, в какую сторону качнется маятник будущих событий, будет зависеть главным образом от решений новой администрации США во главе с Дональдом Трампом.

Евгений Прейгерман
Директор Совета по международным отношениям «Минский диалог»