К вопросу о прочности подводных интернет-кабелей

Джефф Хьюстон

На моем столе лежит трубка. Совсем небольшая. Диаметр каких-то 2 сантиметра на 6 сантиметров в длину. С виду может показаться, что сделана она из обычного белого поликарбоната. Но если посмотреть на срез, оказывается, что пластик лишь оболочка – внутри скрывается медная трубка, а в ней ещё один слой поликарбоната, который окутывает стальную трубку ещё меньшего диаметра. По ней проходит тонкая стальная нить и оптические волокна. Никакой стальной обшивки или каких-либо дополнительных оболочек в трубке нет. Что же это за трубка? Передо мной небольшой кусок подводного оптоволоконного кабеля. Такие используются при прокладке подводных коммуникаций по морскому дну. Почему же они лишены дополнительной защиты? Дело в том, что прокладывают такие кабели на огромной глубине, где, помимо окружающей их воды, особой опасности повреждения нет. Якоря бороздящих морские просторы кораблей и рыболовные снасти обычно до таких глубин не достают. Здесь единственная угроза исходит от подводной сейсмологической активности, но такие случаи крайне редки, да и предсказать их, в любом случае, чрезвычайно сложно. Так что в случае таких подводных толчков оператору всё равно придётся кабель чинить. Если же кабель проходит на меньшей глубине в зонах рыбного промысла, по пути следования кораблей или рядом с портами, его обычно снабжают дополнительными слоями защиты из переплетённой стальной проволоки. Такая стальная оболочка не гарантирует неуязвимость кабеля – якорь крупного судна всё равно может его порвать. Но такая защита не лишена смысла и делает своё дело. Если же нужно максимально снизить риск случайного разрыва кабеля, используется траншеекопатель. С его помощью кабель закапывают в толщу дна, если, конечно, его структура позволяет выкопать такую траншею.

Это, конечно, помогает обеспечить сохранность кабеля и гарантировать его непрерывную работу на небольшой глубине, но полностью исключить возможность разрыва такие меры не позволяют. Разрывы на мелководье всё равно случаются. В конце января вьетнамские интернет-провайдеры сообщили о выходе из строя кабелей AAG (Азия - Америка) и APG (Азия – Тихий океан). Недалеко от Гонконга возникли перебои в работе кабеля AAE-1 (Азия – Африка - Европа), а близ Сингапура что-то пошло не так с Внутриазиатским кабелем. В результате практически одновременно оказались повреждены четыре из пяти подводных кабелей, которыми вьетнамские интернет-провайдеры пользуются для соединения с мировым Интернетом.

На починку подводных кабелей уходят недели, а то и месяцы. Ремонтное судно должно подплыть как можно ближе к месту разрыва, поднять кабель и заменить повреждённую секцию, а затем снова погрузить кабель на дно. Если речь идёт о разрезе в нескольких местах, такую процедуру при-

Рис. 1. Сечение подводного оптоволоконного кабеля.

дётся повторить несколько раз. Обычно специализированные суда и персонал нанимают для починки сразу нескольких кабелей, так что в случае множественных разрывов на ремонт отдельного кабеля может уйти время.

В случае с Вьетнамом во время ремонтных работ оставшийся нетронутым пятый кабель – речь шла о сегменте Сингапур - Вьетнам кабеля SMW-3 – также не работал на полную мощность по состоянию на 22 февраля (https://e.vnexpress.net/news/news/vietnam-s-lastfunctional-undersea-cable-now-malfunctioned-4573176.html) (рис. 2).

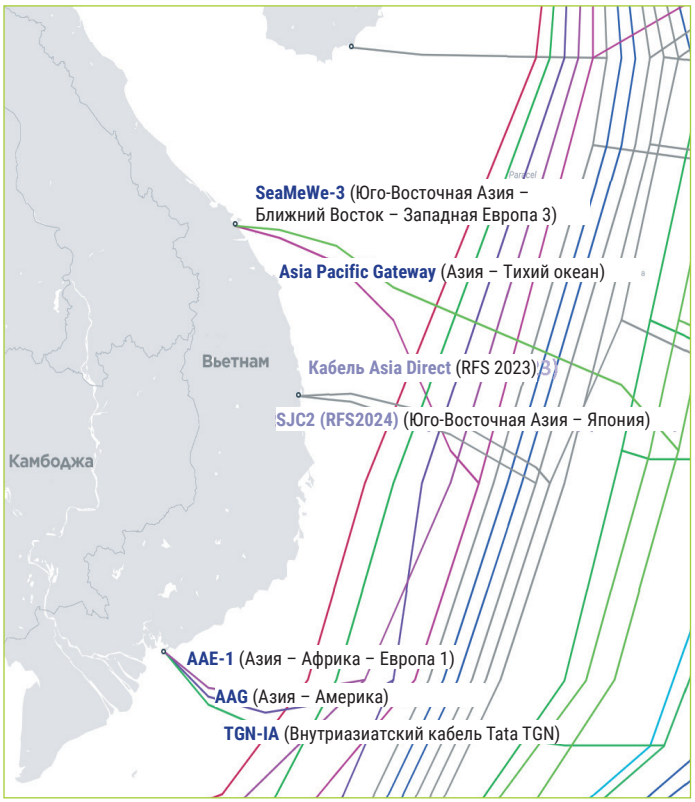
Южно-Китайское море является относительно мелководным. В то же время интенсивность морских перевозок там высокая и ведётся активное рыболовство. Соответственно, инциденты с подводными кабелями вполне возможны, но довольно странно, когда сразу все пять отдельно проложенных кабелей дают сбой. При этом нельзя забывать про политический контекст в этом районе в свете противоречащих друг другу претензий ряда стран на различные участки Южно-Китайского моря (https://en.wikipedia.org/wiki/Territorial_disputes_in_the_South_China_Sea).

С аналогичными проблемами в работе подводных кабелей столкнулся и Тайвань. Два таких кабеля связывают находящиеся вблизи материкового Китая острова Мацзу с Тайванем. По поступившим в конце февраля сообщениям, китайское рыболовецкое судно повредило один из них, а второй пострадал от неизвестного грузового судна (https://www.theregister.com/2023/02/21/taiwan_vietnam_submarine_cable_outages/).

Речь идет о 27-м по счёту повреждении ведущих к островам Мацзу интернет-кабелей за последние пять лет. Повторим, что такое большое число разрывов представляется достаточно нетипичным, если не сказать больше. Можно сослаться на мелководность Тайваньского пролива между Тайванем и островами Мацзу, где глубина составляет около 60 метров. Можно вспомнить, что за несколько лет до этого проводились работы по углублению дна и что это район активного рыболовства и морских перевозок. И тем не менее, такое количество повреждений не может не вызвать подозрений.

Как же обеспечить подключение к Интернету в ситуации, когда существующие интернет-кабели так часто страдают от подобных сбоев?

Рис. 2. Используемые Вьетнамом интернет-кабели (данные Teleglobe).



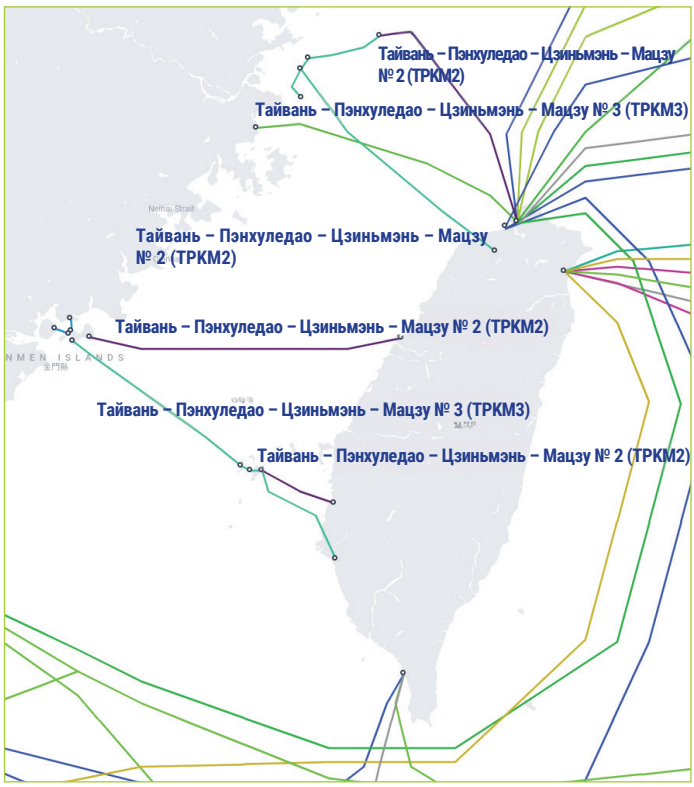


Рис. 3. Интернет-кабели, обслуживающие острова Цзиньмэнь и Мацзу (данные Teleglobe).

Вьетнам пошёл по пути увеличения числа кабелей (https://e.vnexpress.net/news/news/vietnam-toown-three-undersea-cables-by-2025-information-ministry-4570649.html). Речь идёт об ответвлениях, ведущих к кабелю Asia Direct и кабелю Юго-Восточная Азия – Япония 2. Таким образом, конечные точки этих кабелей во Вьетнаме равноудалены от конечных точек существующих кабелей.

История знает множество примеров преднамеренного вывода из строя кабелей связи.

Так, 5 августа 1914 года, через несколько часов после объявления войны Соединённым Королевством против Германии, британское судно разорвало пять немецких подводных кабелей, связывавших Эмден с Виго, Тенерифе, Азорскими островами и США.

В результате Германия лишилась прямой связи с неевропейскими странами, в первую очередь, с США. Пришлось пользоваться альтернативными маршрутами доставки сообщений, но их можно было легко перехватить, поскольку они проходили через Соединённое Королевство.

Вступление США в войну против Германии в 1917 году было во многом обусловлено перехватом так называемой телеграммы Циммермана, в которой речь шла о создании союза между Мексикой и Германией и поддержке нападения Мексики на США. Зашифрованная телеграмма сначала поступила в Копенгаген, а затем в Лондон для последующей передачи в Вашингтон по трансатлантическим кабелям, связывавшим Соединённое Королевство и США. Перехват и расшифровка «телеграммы Циммермана» стали непосредственным результатом разрыва немецких кабелей.

Казалось бы, что мешает подключиться к Гонконгу, до которого совсем недалеко? Но тут возникает вопрос о продолжающихся трениях между США и Китаем. Такое впечатление, что США перестали выдавать разрешения на размещение на своей территории кабельных систем, связанных с Китаем или Гонконгом. Это уже вынудило компании, работающие с большими объёмами данных, такие как Alphabet и Meta (признана в России экстремистской организацией), сконцентрироваться на Сингапуре и сделать его своим главным региональным центром по оказанию услуг. При этом Соединенные Штаты рассматривают всё Южно-Китайское море как зону повышенного риска. Проложенные недавно с участием компаний Google и Meta азиатские интернет-кабели Bifrost и Echo полностью обходят Южно-Китайское море, минуя также Тайвань и Вьетнам (рис. 4 и 5 на следующем развороте).

Если сбои в работе подводных коммуникаций носят случайный характер, то разумным решением представляется увеличение числа кабелей с утолщённой стальной прокладкой и их укладкой в траншеи. Но что, если это преднамеренные акты саботажа? Как может государство защитить свою телекоммуникационную инфраструктуру от преднамеренных действий по выводу её из строя? Если речь идёт о поиске альтернатив подводным кабелям, следует рассмотреть возможность использования радиосвязи.

Микроволновая связь позволяет покрывать расстояние до 150 километров. Это достаточно распространённое решение при передаче информации на средние расстояния в свете её небольшой затратности. Для концентрации радиосигнала между двумя точками можно использовать зеркальные антенны. Двухпунктовая радиосвязь используется по такой схеме уже многие десятилетия и зарекомендовала себя эффективным решением при средних и высоких параметрах широкополосности. Однако такая связь уязвима, поскольку третьи лица могут создавать препятствия для передачи сигнала или глушить его, если злоумышленник создаёт радиосигналы, вносящие помехи в работу оператора микроволновой связи. Но главным недостатком микроволновой связи является её ограниченная дальность. При превышении дистанции в 150 километров приходится отрываться от поверхности Земли и задействовать широкополосную спутниковую связь.

Спутниковая передача данных используется интернет-отраслью уже несколько десятилетий. Возможность её использования для передачи информации на большие расстояния не вызывает сомнений. Такой подход в 1990-е годы активно применяла Австралия, пока шла работа по прокладке подводных кабелей по дну Тихого океана. При передаче сигнала на спутник и обратно возникает нежелательная задержка, но зато таким способом можно сразу охватить целое полушарие. Можно ли как-то препятствовать передаче данных с помощью систем геостационарной спутниковой связи? К сожалению, существует целый набор эффективных способов глушения сигнала. Злоумышленник может направить на приёмник спутника энергоёмкий сигнал, настроив его на ту же частоту, что и оператор связи, что с большой долей вероятности приведёт к выводу системы передачи данных из строя.

Что же касается связи с использованием низкоорбитальных

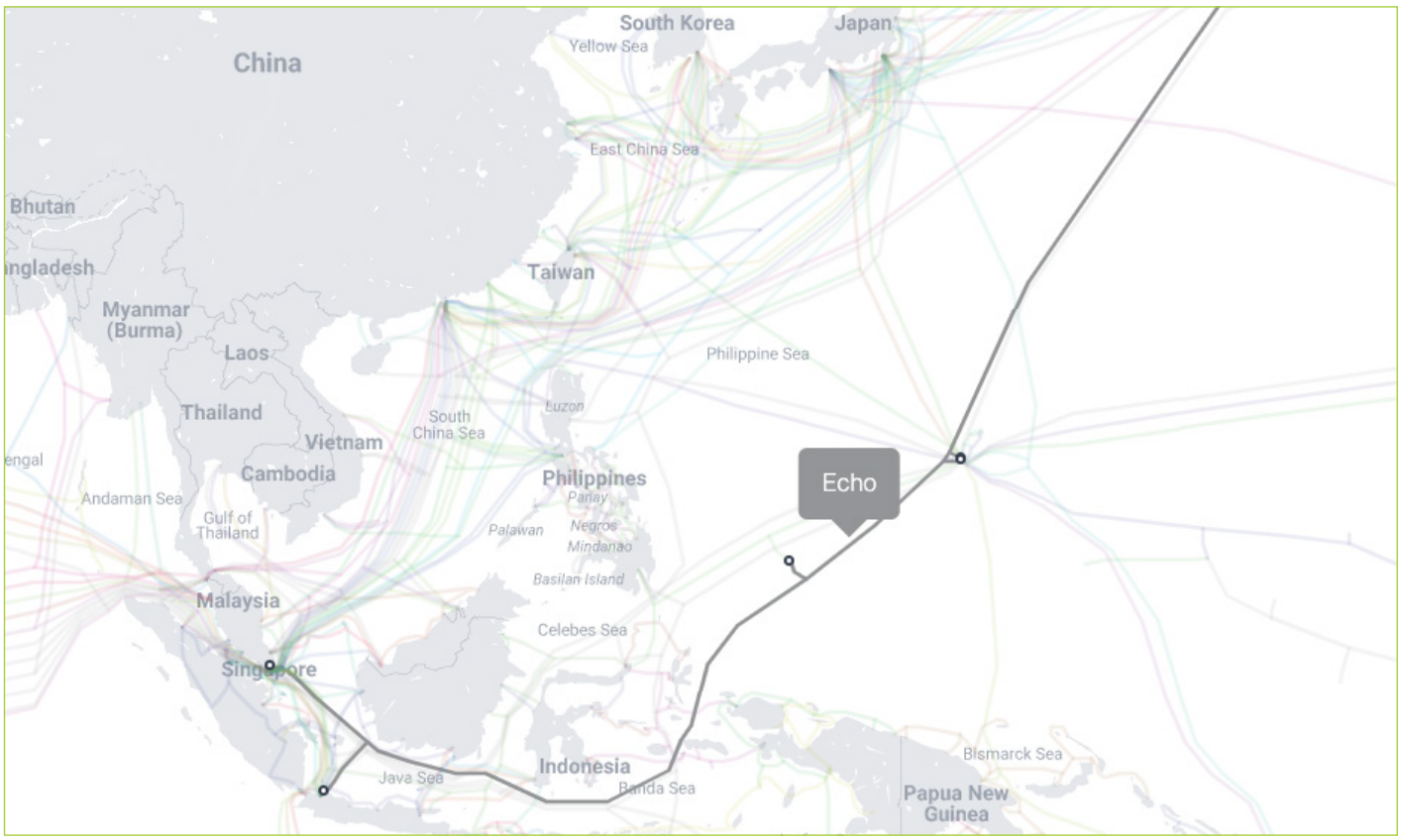


Рис. 4. Маршрут прокладки интернет-кабеля Google Echo (данные Teleglobe).

спутников вместо геостационарных, то в некоторых случаях такое решение представляется целесообразным, и компании O3B и Starlink сейчас оказывают такие услуги во многих странах мира. При этом компания Starlink отдаёт приоритет розничному рынку, тогда как O3B удовлетворяет потребности делового сообщества и государственных заказчиков. Как правило, системы низкоорбитальной спутниковой связи представляют собой достаточно простые решения радиорелейной связи, когда получатель и наземная станция оказываются в «ячейке» одного спутника при его прохождении по орбите. То есть речь идёт об ограниченном диапазоне действия, что имеет как свои преимущества, так и недостатки. В целом это обеспечивает высокую скорость и ёмкость канала спутниковой связи при малой задержке. Учитывая ограниченность зоны покрытия каждого передатчика, для глушения радиосигнала нужно находиться в непосредственной близости либо от пользователя, либо от наземной станции.

По вопросу о низкоорбитальной спутниковой связи важно отметить ещё два важных аспекта. Во-первых, введение в эксплуатацию второго поколения спутников Starlink призвано установить межспутниковые линии связи. Это в некоторой степени затрудняет создание радиопомех, поскольку теперь конечные точки могут и не находиться в пределах определённого расстояния друг от друга. Кроме того, это теоретически расширяет диапазон покрытия услуг низкоорбитальной спутниковой связи, хотя пока конкретных данных от Starlink по этому вопросу нет, так что остаётся только гадать, как будет работать линия межспутниковой связи и как это отразится на оказываемых компанией Starlink услугах в сфере низкоорбитальной спутниковой связи.

Второй вопрос также носит умозрительный характер и состоит в том, сколько всего операторов могут работать в сфере низкоорбитальной спутниковой связи.

Вопрос непростой, поскольку требуется определить, насколько высоко нужно забраться, чтобы выйти из сферы действия суверенного права стран на воздушное пространство и перейти в область «космического права». Согласно договору от 1967 года, ратифицированному более чем ста странами, суверенные права государств на космическое пространство не распространяются. Участвовавшие в составлении этого договора страны не дали чёткого определения самого понятия «космическое пространство» и не прописали, где именно оно начинается. Некоторые страны выступают за точку отсчёта на высоте 100 километров, другие расположили эту границу чуть ниже, на уровне 80 километров, а третьи предлагают считать началом расстояние в 160 километров от поверхности Земли.

Дело в том, что для работы в космическом пространстве операторам систем низкоорбитальных спутников не нужно получать какие-либо разрешения от конкретных стран. Согласование требуется только в отношении используемых ими наземных станций, в связи с чем вопрос об экономической целесообразности низкоорбитальной спутниковой связи во многом обусловлен переговорами о наземной инфраструктуре. Каких-либо общих ограничений на национальном уровне или согласно международным договорам в отношении деятельности государств и компаний в космическом пространстве не существует.

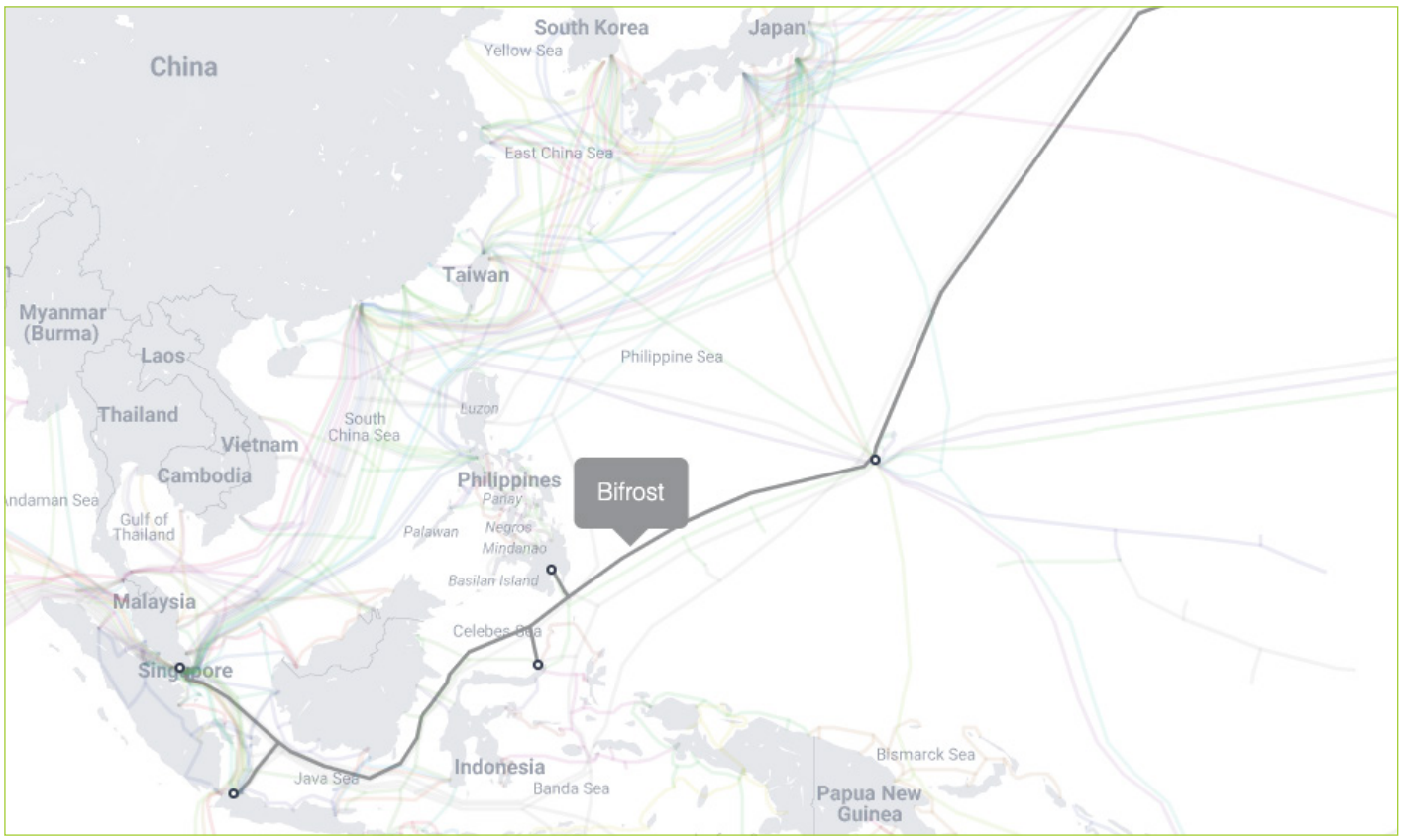


Рис. 5. Маршрут прокладки интернет-кабеля Bifrost (данные Teleglobe).

Если есть ракета-носитель для доставки груза в космос, то далее вы можете делать с выведенными в космос космическими аппаратами всё, что угодно. Несколько десятилетий назад в рамках проекта Iridium было установлено, что главным препятствием в этом отношении выступает получение доступа к частотному спектру в соответствующих странах, чтобы обеспечить приём сигнала на Земле.

К Starlink и O3B теперь решила присоединиться компания Amazon, объявив о планах по созданию спутниковой группировки Kuiper в 3,2 тысячи единиц, которые бы находились на высоте от 590 до 630 километров. В СМИ в течение уже долгого времени регулярно упоминается аналогичный проект Китая на 12 тысяч спутников. В результате, вокруг Земли появится множество низкоорбитальных спутников, в связи с чем важно понимать, что с ними делать после их выхода из эксплуатации. Вопрос космического мусора стоит уже давно. Например, его скопление может вызвать цепную реакцию: при достижении определённого критического объёма такого мусора на определённой высоте можно ожидать непредсказуемых и спонтанных столкновений с действующими спутниками, что повлечёт за собой дальнейшее увеличение объёма космического мусора. Когда космические просторы заполнятся им, это пространство уже никто не сможет использовать, причём достаточно долго.

Поэтому на вопрос о том, способны ли системы радиосвязи стать альтернативой услугам кабельной связи, можно ответить утвердительно. Но радиосвязь тоже не застрахована от попыток целеустремлённых и обеспеченных необходимыми ресурсами злоумышленников помешать её работе. Используемые нами телекоммуникационные системы уязвимы, и полностью гарантировать надёжность таких услуг, идёт ли речь о кабельной или радиосвязи, крайне сложно с технической точки зрения. Построить мощную и общедоступную телекоммуникационную инфраструктуру и при этом обеспечить её абсолютную устойчивость перед лицом обладающего обширными ресурсами и целеустремлённого противника невозможно. А коль скоро мы не в состоянии создать компоненты телекоммуникационной инфраструктуры, полностью защищённой и неуязвимой для попыток препятствовать её работе, нам придётся согласиться с тем, что единственным эффективным решением является создание механизмов, которые вынудят государства сообща отказаться от таких действий путём заключения международных договоров.

Правовая оговорка

Изложенные в данной статье взгляды могут не совпадать с позицией или точкой зрения Азиатско-Тихоокеанского сетевого информационного центра.

Об авторе

Джефф Хьюстон имеет степени бакалавра и магистра наук. Занимает должность ведущего научного сотрудника Азиатско-Тихоокеанского сетевого информационного центра, регионального интернет-регистратора Азиатско-Тихоокеанского региона.

www.potaroo.net