Алексей Лукацкий

ОПРЕДЕЛЕНИЕ ИСТОЧНИКА КИБЕРАТАК

В 5.42 по тихоокеанскому времени сержант военно-воздушных сил США Томас Блейк случайно фиксирует подготовку к пуску баллистической ракеты с территории Китайской Народной Республики. Бывший морпех, только что вышедший в отставку и по стечению обстоятельств оказавшийся на о. Хайнань в сопровождении несовершеннолетней племянницы стремительно проникает на засекреченный китайский объект, пробирается в шахту с ядерными ракетами и с помощью перочинного ножа и курса квантовой физики, со скуки пролистанного в самолете, обезвреживает боеголовку за 7 секунд до старта, в очередной раз спасая мир от глобальной катастрофы. Таким мог бы быть сценарий фильма, посвященного ядерному терроризму и доблестным американским спецслужбам, бойцы которых в одиночку обезвреживают пару сотен китайских экстремистов, решивших развязать третью мировую войну. Но мы живем не в павильонах Голливуда, и я с трудом представляю себе, чтобы желающие развязать глобальный конфликт, если такие найдутся, пошли по этому сценарию. Гораздо более правдоподобным кажется апокалипсис, в котором угроза уничтожения человечества придет из киберпространства. Но если киберинцидент случится, как определить, кто за ним стоит? Ведь даже в реальной жизни установить виновного в преступлении бывает очень непросто.

ЗАЧЕМ НАМ НУЖНА АТРИБУЦИЯ И ЧТО ОНА В СЕБЯ ДОЛЖНА ВКЛЮЧАТЬ

Когда мы имеем дело с миром материальным, в котором присутствуют ядерные боеголовки, воинские формирования, эскадрильи самолетов, боевые группы кораблей, не составляет большого труда определить, кто за ними стоит. Вряд ли стоит ожидать, что авианосная ударная группировка может быть создана олигархом, а шахты с ядерным оружием прорыты любителями. С киберугрозами дело обстоит с точностью до наоборот.

Ситуация усугубляется тем, что в настоящее время по заказу НАТО ведется работа над второй редакцией Таллинского руководства[1] по применению международного права при ведении кибервойн, еще в первой версии которого обосновывалась возможность физического ответа на кибернападение. Очевидно, что в такой ситуации как никогда важна правильная атрибуция источника киберугроз. Ошибочная идентификация может привести к развязыванию войны (локальной, региональной или глобальной) или, наоборот, привести к тому, что будет упущено время, необхо-

димое для подготовки к отражению агрессии. Неспособность установить истинного виновника и, тем более, заказчиков, не позволит в полной мере задействовать имеющиеся в распоряжении каждого государства дипломатические, политические и юридические рычаги.

Поэтому атрибуция нужна не только для того, чтобы понять, кто действует против нас, но и чтобы выстроить оборонительную стратегию и спланировать защитные действия. Один вариант, если мы имеем дело с нарушителем, за которым стоит государство; если же угроза реализована негосударственным *актором*, то и ответные действия должны быть другие. Не на техническом уровне — тут механизмы защиты будут практически одинаковыми (если не рассматривать возможность бомбардировок в ответ на сканирование сети), а на дипломатическом и правовом, и именно от атрибуции будет зависеть набор шагов, которые предпримет государство. В конце концов риск обнаружения и правильной атрибуции может стать сдерживающим фактором для, как минимум, государственных *акторов*.

Говоря об атрибуции, надо заранее понять, насколько точно мы хотим ответить на вопрос *кто нас атакует*, до какого уровня детализации дойти. Таллинское руководство не особо глубоко погружается в детали и просто ищет основания для применения традиционных вооружений против кибернападений, поэтому атрибуция в нем ограничивается определением государства, с территории которого фиксируется кибератака. Однако в условиях, когда любой желающий с любым гражданством может арендовать интернет-сервер в любой стране, ограничиваться только определением местоположения источника атаки было бы некорректно.

Идентификация узла, с которого осуществляется воздействие в киберпространстве, необходима, чтобы понять, принадлежит этот узел частному лицу или организации, какой интернет-провайдер выделил IP-адреса для данного узла (возможно, этот провайдер замечен и в других кибератаках), физическое местоположение данного узла (которое зачастую можно определить), настройки узла, вплоть до используемой операционной системы и приложений, по которым можно попробовать определить языковую или национальную принадлежность атакующего, и т. д.

Идеально, если в рамках атрибуции можно будет сделать вывод о мотивах совершаемых действий, что поможет провести грань между государственными и частными целями совершения кибернападений. Однако определение мотивации — это уже высший пилотаж в области атрибуции спецопераций в киберпространстве. Только техническими средствами решить эту задачу невозможно.

ПОСЛЕДНИЕ ПРИМЕРЫ АТРИБУЦИИ КИБЕРУГРОЗ

Истории с атрибуцией атак встречаются еще на заре формирования отрасли информационной безопасности, но на новый уровень эта тема вышла в 2010 г., когда на комплексе по обогащению урана в иранском Натанзе был обнаружен вредоносный код, позже получивший название *Stuxnet*[2]. Именно тогда специалисты всерьез задумались о том, как идентифицировать силы, стоящие за данным вредоносным кодом. Ведь вирус находился на изолированном от интернета объекте; более того, заражение произошло как минимум за год до начала официального расследования. Иначе говоря, отследить его реального автора ни по интернет-активности, ни по записям журнала прохода на территорию объекта не представлялось возможным. В процессе расследования было высказано предположение

о том, что автором *Stuxnet* являются спецслужбы США и Израиля, что косвенно было подтверждено как разоблачениями Э. Сноудена, так и рядом других публикаций последнего времени. Однако прямых доказательств, которые могли бы быть проанализированы независимыми экспертами, так и не было представлено, что понятно, учитывая специфику объекта и самой ситуации.

И до, и после *Stuxnet* бездоказательные заявления об атаках со стороны различных государств делались в рамках конфликтов в Северной Осетии, Югославии, Украине, Ливии, Сирии и т. п. Но масла в огонь подлила американская компания *Mandiant*, позже купленная *FireEye*[3], также американской. За последнее время *FireEye* выпустила несколько отчетов, в которых подробно исследуются различные кибершпионские и хакерские кампании, например, действия китайской хакерской группы *APT1* (в качестве одного из атрибутов называлось время максимальной активности, совпадающее с часовым поясом Шанхая), российской хакерской группы *APT28*, иранской группы *Ajax Security Team*, взлом *Sony Pictures Entertainment*.

Помимо *FireEye* аналогичные исследования проводились компаниями:

- *Cylance*[4], которая изучала кампанию иранских хакеров *Cleaver* (*нож мясника*);
- *Partners*, которая раскрыла операцию *Newscaster* (*телекомментатор*), также исходившую из Ирана;
- *Лабораторией Касперского*, которая раскрыла кампании *Маска*[5] и *Красный октябрь*;
- *Group-IB*[6], нашедшей след *Исламского государства* в атаках на многие российские организации;
- *BAE Systems*, исследовавшая атаки на украинские компьютеры и нашедшая на них *русские* отпечатки;
- *Check Point*, раскрывшая ливанскую хакерскую группу *Volatile Cedar* (*Летучий кедр*);
- *Taia*[7] *Global*, которая вопреки распространенному мнению, что компанию *Sony* взломали хакеры из Северной Кореи, *доказала*, что *Sony* все-таки атаковали из России.

Во всех случаях для атрибуции использовались различные обоснования. Например, в марте 2014 г. американская *BAE Systems* обнаружила на украинских компьютерах следы проникновения *хорошо подготовленных профессионалов*, использующих вредоносное ПО *Snake*[8] (*Змея*) из часового пояса, в котором находится Москва (почему была названа Москва, а не, например, Йемен, Ирак, Мадагаскар или Эфиопия, находящиеся в том же часовом поясе?). Позже тот же вредоносный код был найден на нескольких компьютерах бельгийского МИДа. Затем *русский след* был обнаружен финской компанией *F-Secure* во вредоносном коде *BlackEnergy*, а там подоспел и отчет *FireEye* про хакерскую группу *APT28*, действующую из Москвы и пишущую вредоносные программы в рабочее время по Москве. Видимо, это проявление классических для иностранцев стереотипов: Россия — это Москва и одна страна — один часовой пояс.

В случае с атаками ИГ на российские ресурсы атрибуция была достаточно простой: группировки *Cyber Caliphate*, *Team System Dz*, *FallaGa Team* и *Global Islamic Caliphate* массово взламывали интернет-ресурсы с хорошей посещаемостью, на которых размещали свои лозунги и мгновенно публиковали информацию об этом в социальных сетях *Twitter* и *Facebook*. По этому сценарию действовала и *Сирийская электронная армия*. Примерно также идентифицировались и действия *КиберБеркута*, который

не скрываясь публиковал данные о своих *подвигах* на своем сайте, что облегчало поиск виновных. Самый простой способ атрибуции кибернападений — добровольное признание в содеянном авторов атаки. При условии, правда, что учетные записи или ресурсы, на которых размещаются признания (*Twitter*, *Facebook*, сайт и т. п.), действительно принадлежат им, а не просто взломаны кем-то другим.

DDoS-атаки Ирана против финансовых институтов США (операция *Ababil*[9]) и топливно-энергетических компаний Катара и Саудовской Аравии в конце 2012 — начале 2013 гг. были идентифицирована по регистрации используемых для атаки IP-адресов.

Операция иранских хакеров *Нож мясника* была атрибутирована сразу по ряду параметров. Во-первых, в рамках операции использовались персидские имена хакеров, а во-вторых, домены, IP-адреса и инфраструктура, используемые в рамках атаки, были зарегистрированы в Иране. Также и действия ливанского *Летучего кедра* были идентифицированы по нескольким параметрам: командным серверам, расположенным на площадке ливанской хостинговой компании, по DNS-запросам, которые вели в Ливан, и адресам электронной почты, на которые были зарегистрированы некоторые домены и которые были связаны с ливанскими политическими активистами. Очевидно, чем больше различных параметров используется для атрибуции, тем она точнее.

Конфуз случился в истории с проникновением в сеть компании *Sony* в ноябре 2014 г., которое и послужило причиной очередного витка серьезного внимания США к теме кибербезопасности и разработки целого пакета нормативных актов, направленных на усиление борьбы с хакерами. США практически сразу обвинили в атаке на *Sony* северокорейских хакеров, которые предупреждали, что за выпуском в прокат фильма *Интервью* про северокорейского лидера Ким Чен Ына последуют ответные действия. И хотя *после* не значит *вследствие*, американские власти поспешили назвать виновника всех бед, попутно введя против Северной Кореи очередные санкции. И снова доказательства участия в деле корейских злоумышленников добывала *FireEye*. Однако американская корпорация *Taia Global* поставила под сомнение выводы *FireEye* о северокорейском следе, представив доказательства, что за атаками на *Sony* стоят россияне. Финальный аккорд в этой истории пока так и не прозвучал.

ПОЧЕМУ ВСЕ ТАК ПЛОХО С ОПРЕДЕЛЕНИЕМ ИСТОЧНИКА КИБЕРУГРОЗ?

Можно выделить несколько групп факторов, которые мешают адекватному и однозначному определению источников спецопераций в киберпространстве: геополитические, правовые, технические, экономические и психологические.

Геополитическая ситуация

Кибератаки военного назначения сегодня превратилась в инструмент геополитической борьбы. Что может быть проще, чем обвинить то или иное государство в агрессии только на том основании, что с его территории зафиксирована кибератака? И, как мы неоднократно наблюдали за последнее время, отдельные страны и блоки стран активно используют этот прием. Кто взломал Пентагон? Русские хакеры. Кто взломал Белый дом и получил доступ к переписке Барака Обамы? Русские хакеры! Кто взломал лабораторию в Лос-Аламосе, занимающуюся разработками

ядерного оружия? Опять русские хакеры! Так и формируется имидж всесильного, но почему-то неуловимого русского хакера, который ломает все, что попадется ему под клавиатуру. Правда, Россия тоже не отстает, регулярно заявляя об атаках, идущих с территории Украины или Грузии (в зависимости от напряженности во взаимоотношениях с тем или иным бывшим *партнером* по Советскому Союзу). Недавно стало известно, что Россию активно атакуют представители *Исламского государства*, выбравшего наше государство в качестве очередной жертвы.

Желание связать конкретную атаку с конкретным государством, не разбираясь в реальных источниках и причинах, вполне объяснимо — это удобный прием в геополитической борьбе, особенно если нужно быстро создать образ врага. Да и подпитывать его несложно: достаточно на очередной пресс-конференции вскользь упомянуть про *русский*, *исламский*, *украинский* след, и журналисты сами раздуют вокруг этого заявления *киберпожар*.

Отдельно стоит упомянуть, что идентификация источника в сложной атаке, проходящей через несколько государственных границ и континентов, требует активного взаимодействия представителей государств, не только находящихся в разных юрисдикциях, но иногда и агрессивно, даже враждебно по отношению друг к другу настроенных. Можно ли быть уверенным, что такое сотрудничество будет налажено? Далеко не всегда. Например, не так давно на конференции *Positive Hack Days* в Москве представители ФСБ заявили, что в настоящий момент большая часть хакерской активности, направленной против России, идет с территории Украины, но нормально взаимодействовать с украинскими спецслужбами не удается по вполне понятным причинам. Хотя иногда наблюдается и обратная картина. Например, во время подготовки и проведения зимних Олимпийских игр в Сочи американские и российские спецслужбы достаточно активно взаимодействовали в рамках обеспечения безопасности игр. И это несмотря на уже произошедшее охлаждение дипломатических отношений, заморозку отдельных контактов и приостановление ряда рабочих групп.

Неразбериха в международном праве

Новый порядок мироустройства, а вместе с ним и принципы обеспечения международной безопасности, сформировавшиеся по итогам Ялтинской и Потстдамской конференций, строились на двух ключевых понятиях — *война* и *агрессор*, которые в современном мире морально устарели. Согласно общепринятой теории, субъектами войны и агрессорами признаются целые государства: Ирак, Ливия, Сирия, Россия, Саудовская Аравия, США. А что делать с незаконными вооруженными формированиями, например, в ДНР и ЛНР? А с международными террористическими организациями, такими как *Аль-Каида*, *Исламское государство*? А иные негосударственные *акторы*, которые могут осуществлять те или иные спецоперации, несущие не меньшую угрозу, чем иные государства? Как квалифицировать действия, осуществляемые киберанархистами и иными группами с приставкой *кибер-*: *Anonymous*, *LulzSec*, *КиберСотня*, *КиберБеркут*? Это агрессия или нет? Действуют такие киберанархисты самостоятельно или они направляются и финансируются государственными структурами, желающими снять с себя ответственность и переложить ее на якобы неуправляемых хакеров? Таллинское руководство отвечает на эти вопросы утвердительно, приравнивая всех, кто действует с территории какого-либо государства, к самому государству.

По сути, мы находимся на пороге нового технологического уклада, который потребует серьезного пересмотра всей системы международного права и расширения ее сферы охвата для регулирования информационных технологий. Сегодня в международном праве зафиксированы основные принципы взаимодействия именно государств и именно в *материальных* пространствах: наземном, воздушном, морском, космическом. И только отношения в киберпространстве остаются практически нерегулируемыми. До сих пор не существует даже общепринятого определения киберпространства. Нелюбовь представителей российских властей к приставке *кибер* — это отдельная тема. Правда, так нелюбимый МИДом термин *кибербезопасность* активно используется многими российскими организациями, включая госкорпорации. Знаете ли вы, сколько раз ООН образовывала и расформировывала специальные комиссии, которые должны были определиться с более привычным для нас термином *терроризм*? Более 30. А утвержденного термина до сих пор нет. Так чего же мы хотим в отношении термина *киберпространство*?

Особую соль всему этому придает отсутствие в киберпространстве географической привязки, что отличает его от театров ведения традиционных военных операций. В качестве примера достаточно взять эту статью, которая, не выходя за пределы моего компьютера, успела попутешествовать по миру: я начинал ее писать в Киеве, продолжил в самолете над Тихим океаном, в Челябинске, а закончил уже в Сочи. Что же считать местом создания этого *нематериального материала*? Ровно так же все обстоит и с кибератаками. Почему-то их источником считается компьютер, с которых зафиксировано обращение к атакуемым ресурсам. А ведь он может быть только последним в цепочке, насчитывающей 2, 5, 10 узлов. А как трактовать ситуацию, когда атака действительно осуществлялась с компьютера, например, в России, но он был взломан и использован как промежуточная площадка? Будет ли владелец взломанного компьютера, сам жертва, нести ответственность за действия, о которых он даже не подозревает?

Интернет-анархия

Не будем лукавить, интернету до сих пор присуща определенная анархия. Отсутствие четких определений, общепринятых правил и стандартов по мониторингу, учету и обмену трафиком, постоянные разговоры о *privacy* — все это не способствует созданию среды, в которой можно было бы однозначно проследить за каждым сетевым пакетом или сессией. А высокие скорости передачи данных приводят к тому, что они хранятся очень непродолжительное время, за которое сложно отследить злоумышленника.

Технические сложности

Технические причины лежат в основе невозможности простого определения источника атак в киберпространстве, причем независимо от формы их реализации — в виде DDoS-атак, путем проникновения через защитные препоны, в виде рассылок вредоносного кода через электронную почту или путем заражения сайтов и флешек, через которые вредоносное ПО попадает во внутреннюю сеть предприятия.

В 1960–1970-е гг., когда создавались протоколы, положившие начало современному интернету, никто не задумывался о необходимости однозначной идентифи-

кации всей цепочки передачи пакетов данных из точки А в точку Б. Более того, сама по себе технология работы интернета подразумевает децентрализацию и распределенность. И то, что устраивало всех последние 40 лет, сейчас стало играть с нами дурную шутку. Как определить реального автора пришедшего мне на компьютер сетевого пакета, если технически возможно изменить адрес отправителя? Текущая, четвертая, версия протокола IP в принципе не подразумевает однозначной идентификации и аутентификации инициатора соединения (хотя разговоры об интернет-паспортах и идентификации всех, кто входит в интернет, ведутся давно). Правда, это не мешает официальным лицам и представителям военных структур заявлять об идентификации источника атаки.

Но отсутствие в текущей версии протокола IPv4 необходимых атрибутов для определения местоположения источника атаки — не единственное препятствие. Никто не может помешать злоумышленнику, желающему скрыть свое истинное местоположение, использовать любой имеющийся в интернете прокси-сервер (сервер-посредник) или анонимайзер. В случае реализации атаки через них мы увидим в качестве адреса источника атаки не реальный адрес злоумышленника, а адрес сервера-посредника. Как быть в таком случае? А ведь такие сервера во множестве разбросаны по разным национальным сегментам интернета. Находясь в Пекине, я могу реализовать атаку через посредника в Москве, Гаване, Рейкьявике или Гонолулу.

Ситуация усугубляется тем, что я могу арендовать специальные сервера (так называемый abuse-устойчивый хостинг), которые будут целенаправленно скрывать мой истинный адрес. И таких промежуточных серверов может быть много — 2, 5, 10, 100. В такой ситуации атака обладает динамически меняющимися пространственными характеристиками, что коренным образом отличает ее от обычных наступательных вооружений. Может ли ядерная боеголовка динамически менять свое местоположение? Да, но очень медленно, если возить ее на специальном автотранспорте или поезде. Но и в этом случае ее географические координаты ограничены границами одного государства, в крайнем случае блока. Для кибератаки поменять за несколько минут или даже секунд географическую привязку и числиться на разных континентах в порядке вещей.

Аналогичная ситуация возникает, и если подняться выше по так называемому стеку интернет-протоколов и посмотреть на электронную почту, которая может содержать угрозы или реальный вредоносный код. Идентифицировать настоящего отправителя почты, если он того не желает, практически невозможно. Для этого надо пройти по цепочке всех узлов, через которое проходило почтовое сообщение и которые могут находиться в разных странах и юрисдикциях.

Отдельный вопрос с файлами и вредоносным программным обеспечением. В них нет печати и, как правило, не стоит подпись автора, который желал бы оставить след в истории. Поэтому исследователям приходится просматривать огромные объемы информации в поисках *зерен правды*, позволяющих с определенной долей вероятности определиться с источником атаки. Например, в рамках расследования операции *Нож мясника* компания *Cylance* собрала и изучила свыше 8 Гб данных, 80 000 файлов, журналы регистрации на узлах жертв и т. п. И только после этого она смогла заявить об иранском следе, и то с оговорками. Однако технический анализ так и не смог дать ответ на вопрос, стояло за этой операцией государство или это была частная инициатива.

Бизнес превыше всего

Какая задача стоит перед коммерческим предприятием, которое подверглось кибернападению? Долго и мучительно собирать доказательства или быстро вернуться в рабочее состояние и продолжить прерванные операции? Почему ИТ-директора многих коммерческих и государственных организаций любят подменять термин *информационная безопасность* термином *непрерывность бизнеса*? Да потому что задача любой организации будь то министерство, электростанция, система управления вооружениями, банк, — обеспечить непрерывное функционирование и бесперебойность работы всех своих сервисов. А если и произошел какой-то сбой, надо как можно скорее перегрузить сервер, переустановить операционную систему, переключиться на резервный канал. Мало кого интересует полноценное расследование с атрибуцией, которое может и не принести ожидаемого результата, поэтому концепция современной защиты заключается в улучшении защитных киберстен, отражении атак и их локализации, если они все-таки проникли в сеть предприятия. Задачу расследования и атрибуции мало кто перед собой ставит. И это я еще не рассматриваю ситуацию, когда организации сознательно мешают расследованию, не желая, чтобы их связывали с кибератаками или обвиняли в слабой защищенности, которая и послужила причиной успешного проникновения.

Психология и отсутствие компетенций

В психологии известен факт, что непонятное часто вызывает опасение и неприятие, не надо забывать и о некоторой инертности госаппарата, поэтому естественно, что новые понятия и технологии входят в официальный дискурс с некоторой задержкой. Достаточно посмотреть на текст действующей военной доктрины РФ, и мы увидим, что используемые в ней термины *военный конфликт*, *локальная война*, *региональная война*, *крупномасштабная война* не применимы в киберпространстве.

Кроме того, в большинстве государств (и тут Россия не исключение) на высших должностях находятся люди, привыкшие оперировать понятиями, традиционно использующимися в описания наземных, воздушных, морских или космических пространств, но не применимыми к киберпространству. Отсюда постоянные ляпы, допускаемые даже в самых новых документах по рассматриваемой теме. Те, кто могли бы объяснить ошибочность такого подхода, не допускаются к разработке этих документов. А если их и допускают, то к мнению этих *безусых младенцев* не всегда прислушиваются.

Есть и другая составляющая данной проблемы. Достаточно вспомнить, какой путь прошли мировые державы, вырабатывая основы ядерного сдерживания. Доверие доверием, но не стоит забывать про *доверяй, но проверяй*. Дипломатические контакты, многостороннее сотрудничество, дорожные карты, выработанные процессы и процедуры позволили если не гарантировать, то с высокой степенью уверенностью утверждать, что то или иное государство не проводит (или, наоборот, проводит) ядерные испытания, а также сокращает стратегические наступательные вооружения (договоры СНВ I, РСМД и т. д.). Хотя в последнее время что российские, что американские дипломаты регулярно утверждают, что противоположная сторона нарушает взятые на себя обязательства. И непонятно, есть у них реальные доказательства или мы имеем дело просто с геополитической риторикой. В международной информационной безопасности, история которой насчиты-

вает всего чуть больше 20 лет, такого опыта нет. Более того, иногда складывается впечатление, что отдельные государства специально не идут навстречу, чтобы скрывать свой потенциал в этой сфере.

КАК МОЖНО ОПРЕДЕЛИТЬ УЧАСТНИКОВ СПЕЦОПЕРАЦИЙ В КИБЕРПРОСТРАНСТВЕ

Хорошо, с проблемами мы разобрались. Но как же все-таки *Group-IB*, *Лаборатория Касперского*, *Cisco*, *Cylance*, *Taia* и другие проводят свои расследования и делают выводы об источнике атак? Обычно в качестве доказательств используются следующие индикаторы (признаки):

Место регистрации IP-адресов и доменов, участвующих в атаке или предоставляющих инфраструктуру для реализации атаки. При этом анализируется не только страна регистрации, но и сопутствующая информация, которая может быть получена с помощью сервиса WHOIS: ФИО владельца домена или IP-адреса, его контакты. Все это позволяет при превышении определенного порогового значения сделать вывод о стране, которая *стоит за кибернападением*. Если же злоумышленник не очень квалифицированный, можно идентифицировать и физическое место расположения источника атаки. Правда, это может оказаться интернет-кафе или библиотека, но даже такая *точность* лучше, чем просто *стрелять в белый свет, как в копеечку*, даже не пытаясь установить физическое местонахождение инициатора кибератаки.

Трассировка атаки до ее источника или хотя бы локализация области, в которой источник находится. Такой функционал есть у многих маршрутизаторов, на которых построен интернет. Помимо механизма *Traceback*, использующегося на сетевом оборудовании, для идентификации злоумышленников могут быть использованы фильтрация трафика на интерфейсах маршрутизатора (ingress filtering), протокол ICMP для возврата отброшенного на жертву трафика обратно его инициатору. Например, в случае шпионской кампании *Лунный лабиринт (Moonlight Maze*[10]*)*, направленной против ВПК США, НАСА и ряда американских государственных структур, отследить организаторов удалось именно путем анализа обратного маршрута до серверов, зарегистрированных в России (правда, связь с государственными структурами так и не была установлена). Аналогичный метод, правда, в более сложном варианте, позволил сделать вывод о том, что за хакерской кампанией *Аврора*, в рамках которой были атакованы многие технологические компании США (например, *Google*, *Juniper*, *McAfee*, *Adobe* и т. п.), стоит Китай.

Временные параметры. Как показали ранее приведенные примеры, нередко исследователи анализируют время создания вредоносного кода, время начала операции в киберпространстве или время наибольшей активности. Пусть и с оговорками, но эта информация может служить основой дальнейшего анализа. И хотя она не укажет на конкретного нарушителя, она позволит сузить число стран, которые могли бы быть причастны к анализируемой ситуации.

Анализ программного кода, в котором могут быть найдены комментарии, ссылки на сайты, домены, IP-адреса, которые участвуют в атаке. Анализ функциональности программного кода позволяет сузить число возможных нарушителей. Например, анализ кода *Stuxnet* показал, что для его создания надо было не только знать, как работают центрифуги IR-1 в Натанзе, но и иметь стенд для проверки работоспособности вредоносного кода, который позже вывел из строя большое количе-

ство центрифуг по обогащению урана. Но многие ли *актеры* способны приобрести центрифуги для тестирования? Это позволило существенно снизить число возможных нападавших, а дополнительные сведения позволили даже назвать государства, которые стояли за разработкой *Stuxnet*, — США и Израиль.

Помимо изучения фрагментов кода, отдельные исследователи пытаются даже ***изучать почерк программистов и определять по нему школу программирования***: американская, русская, китайская и т. п. Хотя пока это скорее из области фантастики и плохо формализуемо. Однако уже сейчас известны отдельные работы в части автоматизации и алгоритмизации процесса определения почерка программиста для дальнейшего использования этой информации в расследовании и атрибуции.

С анализом почерка тесно связана и лингвистика, а точнее ***стилометрия***, которая ***позволяет определить стилистику языка в тех же самых комментариях или сопутствующих текстах***. Известно, что то, в какой стране родился человек, в какой культуре рос, в какой языковой среде воспитывался, определяет его стиль письма, который можно выделить и зафиксировать. Например, выросший в России или Советском Союзе человек, позже уехавший в Великобританию или США, никогда не будет говорить на языке так же, как коренной англичанин или американец. Эти различия позволили, например, специалистам компании *Taia Global* сделать вывод о том, что за атаками на *Sony* стоят не северокорейские, а русские хакеры. Аналогично эксперты *Лаборатории Касперского* предположили, что за шпионской кампанией *Маска* стоят испаноговорящие хакеры. Причиной такого вывода послужило использование в коде испанских слов и сленга, которые никогда не используется англоговорящей аудиторией.

Обманные системы или honepot/honeynet — популярный в свое время инструмент, интерес к которому со временем поугас, а сейчас возвращается вновь. Идея проста: в сети запускается фальшивый, подставной узел, который злоумышленник атакует, оставляя следы своей несанкционированной активности, — вот ее-то и изучают эксперты.

Еще один метод — ***оперативная разработка***. Он мало чем отличается от того, что мы знаем из боевиков или детективов. Внедренные агенты, *стукачи*, *сочувствующие* и другие источники информации позволяют идентифицировать или хотя бы сузить спектр возможных акторов, стоящих за той или иной атакой. Хороший пример — Эдвард Сноуден, который успел рассказать немало интересного о деятельности спецслужб, в которых ему довелось служить.

Анализ активности на форумах и в социальных сетях. Именно так в 2007 г. была выяснена причастность молодежного движения *Наши* к атакам на ряд эстонских ресурсов. Однако связь *Наших* с российскими властными структурами в данном конфликте так и не была подтверждена. Аналогичным образом после публикации ролика на *YouTube* иранской хакерской группировки *Izz ad-Din al-Qassam Cyber Fighters* была *доказана* роль иранских хакеров (но не самого государства) в атаках на американские банки. Наконец, Сирийская электронная армия регулярно берет на себя ответственнось за атаки на отдельные американские ресурсы. Например, именно они заявили о взломе учетной записи в *Твиттере агентства Assocaited Press*[11], в котором написали о взрыве в Белом Доме и ранении Барака Обамы. Анализ активности хакеров и оперативная разработка — единственные методы определения мотивов кибератаки. Ни анализ IP-адресов, ни лингвистика не дают возможности ответить на вопрос *почему*, ограничиваясь только ответом на вопрос *кто*.

В отдельных случаях *автора* ***можно идентифицировать постфактум по его действиям***. Речь идет не только о том, что он осознанно или случайно делится фактом своего участия в атаке в социальных сетях. Например, в случае вторжения в интернет-банк, кражи денег и перевода их на подставные или реальные счета, наблюдая за владельцем счета, можно выйти и на тех, кто стоит за ним или кто его нанял. Также украденная информация может появиться на аукционах и биржах, публичных и закрытых. Дальше следователи могут вступить в переговоры с продавцом и провести его атрибуцию или получить важную информацию для дальнейшей атрибуции кибернападения.

Из всего вышесказанного следует, что универсального и 100-процентного метода не существует. Более того, далеко не всегда техническими методами можно ограничиться. Например, когда в 2012 г. стало известно об атаке вредоносного кода *Gauss* на ливанские банки, многие эксперты задавались вопросом *а зачем это было нужно?* Неужели нет более лакомых кусков, чем ливанские банки? И, поскольку технические методы не помогли провести правильную атрибуцию, пришлось использовать косвенные признаки. Например, по анализу функций кода *Gauss* исследователи предположили, что он направлен на изучение счетов организации *Хезболла*, которая таким образом отмывала деньги, что и интересовало тех, кто стоял за атакой на финансовые институты Ливана. А, учитывая, что *Хезболла* признана террористической организацией в ограниченном числе стран (в частности в США и Израиле), спектр возможных инициаторов был сужен до пары государств.

Наверное, только полная перестройка архитектуры интернета помогла бы решить эту проблему с технической стороны. Но это недостижимая, а может быть, и вредная мечта. Остается только совершенствовать указанные технические рецепты, обильно сдабривая их правовыми и дипломатическими приправами, позволяющими с большей уверенностью утверждать, что правильная атрибуция инициаторов спецопераций в киберпространстве возможна. Неслучайно из американской разведки вышел широко используемый в расследовании киберпреступлений термин *OSINT (open source intelligence)*, т. е. поиск, сбор и анализ информации, полученной из открытых источников. Сегодня без активного развития и использования инструментов *OSINT* сложно эффективно заниматься атрибуцией спецопераций в киберпространстве, а эта техника требует высокой квалификации лиц, которые участвуют в определении источника кибернападения. Это могут быть как сотрудники служб информационной безопасности государственных органов и критически важных объектов, так и представители правоохранительных и силовых структур, уполномоченных проводить оперативно-розыскную деятельность в киберпространстве.

Определенным подспорьем в атрибуции кибератак может служить так называемая *Q-модель*[12], разработанная Томасом Ридом и Беном Бухананом из Королевского колледжа Лондона и позволяющая взглянуть на процесс идентификации акторов в киберпространстве как бы с высоты птичьего полета. Множество наводящих вопросов помогают правильно сформулировать задачу расследования и более оперативно найти виновника, стоящего за той или иной атакой.

ДОВЕРЯЙ, НО ПРОВЕРЯЙ, ИЛИ ЧТО ДАЛЬШЕ?

Допустим, мы смогли определить источник кибератаки. Но что делать дальше? Вспомним историю с атаками типа *отказ в обслуживании* (DoS) на эстонские интернет-ресурсы и взломы веб-сайтов этого прибалтийского государства. Как

член НАТО Эстония обратилась к Североатлантическому альянсу за помощью. Но Альянс не смог ничем помочь — ни отреагировать на эти атаки, ни сформулировать позицию, является ли такое *нападение* в киберпространстве угрозой для членов Альянса. И что это было — спланированное нападение или действия патриотически настроенной молодежи? Именно эти события послужили определенным толчком к созданию Таллинского руководства, которое оправдывало бы применение традиционных и понятных для НАТО вооружений в ответ на кибератаки. В настоящее время готовится вторая редакция этого руководства, которая должна найти еще больше оснований для уравнивания физических и кибернападений. Но мало кто может ответить на вопрос *«А что дальше?»*.

Как из журнала регистрации сетевого оборудования и средств защиты сделать вывод об умысле? Умысел подразумевает осознание опасности деяния лицом, которое его совершает. И если в рамках атрибуции атак мы смогли определить лицо и даже собрать доказательства, неоспоримо доказывающие, что именно оно стояло за атакой в киберпространстве, этого недостаточно для начала каких-либо юридических разбирательств, особенно таких, которые могут повлечь за собой серьезные последствия вплоть до вооруженного противодействия. Вспомним 2003 г., когда на атомной электростанции в США появился вредоносный код, занесенный на флешке, что привело к выходу системы управления из строя и отключению электростанции с последующим веерным отключением каскада электростанций на всем восточном побережье. Результат — многочасовое отключение электричества у сотен тысяч американцев. Что это было? Случайность или целенаправленное воздействие? Был ли в этом злой умысел? А если был, то чей — сотрудника АЭС, подрядчика, террористической группировки *Аль-Каида*, китайского правительства? Спустя 11 лет, в декабре 2014 г., была проведена атака на южнокорейскую атомную корпорацию KHNP[13]. Если судить по тем действиям, что были зафиксированы специалистами атакованной АЭС, имела место целенаправленная атака (корейцы называют ее террористической). Но авторство кибернападения опять остается неизвестным.

Допустим, проведя атрибуцию какой-либо атаки, мы смогли обнаружить, что *автором* у нас является физическое лицо, совершающее свои действия с целью наживы, вандализма или просто по идеологическим мотивам. Методов правовой защиты жертвы существует немало. Можно обратиться в правоохранительные органы, можно подать иск в суд, можно выписать ордер на арест. Следователи и эксперты проведут расследование, возможно, изымут компьютерную технику и иные доказательства из квартиры подозреваемого и сделают вывод о том, что это именно он совершил деяние, квалифицируемое одной из статей Уголовного кодекса Российской Федерации. А судья посчитает, что арестованный хакер оступился, *не ведал, что творит* и отпустит, в лучшем случае оформив условный срок. Таковы российские реалии. За пределами России в зависимости от государства суды могут быть более продвинутыми в части признания отдельных физических лиц виновными в совершении компьютерных преступлений.

Проблемы начинаются, если преступник находится за пределами государства, в котором располагается жертва. В таких случаях американские власти иногда просто выкрадывают подозреваемого и предъявляют ему обвинение на своей территории, но такие варианты я не рассматриваю, так как они выходят за рамки правового поля. Остается только объявлять подозреваемого в международный розыск, оформлять запрос в *Интерпол* и просить его выдачи у государства, с которым заключены соответствующие договора. И вот тут возникает вопрос, на который универсально-

го и сформировавшегося ответа пока нет. Что должно послужить доказательством в суде, чтобы он выдал соответствующий вердикт в отношении киберпреступника? В мире, насколько мне известно, нет примеров судебных разбирательств, в которых бы активно использовались доказательства, собранные в рамках атрибуции кибернападений. Даже в случае с террористами или финансовыми мошенниками ситуация с выдачей обстоит не так просто, что уж говорить о хакерах.

Если *актором* у нас является отдельная компания, то ситуация с ней по части процедуры схожа с той, что применима к физическим лицам. Но тут прецедентов нет вообще, даже в рамках локального законодательства. Я не помню случаев, чтобы какую-либо компанию или ее руководство осудили за компьютерные преступления. В мире, возможно, такие ситуации и имели место, но и их я тоже не припомню.

Можно предположить какой ответ ожидается в отношении террористической группировки или хакерской группировки, даже если прошла их успешная атрибуция. Многие из них известны не один год (даже десятилетия), но продолжают существовать и творить свои черные дела. То же *Исламское государство*, которое стоит за многими последними нашумевшими атаками и даже открыто признает их. Вспомним, что ООН до сих пор не смогло прийти к согласию по выработке термина *терроризм*. Как можно привлечь *Исламское государство* к ответственности за кибернападения?

А теперь попробуем представить себе, что *актором* является государство. Есть ли шансы довести такого рода инциденты до некоего логического конца? Инцидент со *Stuxnet* был зафиксирован 5 лет назад — и что? Иран обратился в какой-нибудь международный суд, чтобы обвинить США или Израиль в совершении нападения на ядерный объект? Американцы постоянно обвиняют Китай в совершении кибератак на свою инфраструктуру, но это не мешает обеим сторонам усиливать экономическое взаимодействие.

Почему так происходит? Мне кажется, тому несколько причин, и все они носят правовой, экономический и политический характер. Во-первых, непонятно, какой суд должен рассматривать дела об атрибуции кибернападений и имеют ли необходимую квалификацию судьи существующих международных судов. ЕСПЧ? Постоянная палата третейского суда? Суд Евросоюза? Международный уголовный суд в Гааге? Или Международный суд ООН? Но все они используют при рассмотрении дел и вынесении решений международные конвенции и договора, международные обычаи, общие принципы права. Но ничего из перечисленного не применимо к киберпреступлениям.

Например, статья 51 Устава ООН говорит о праве на коллективную или индивидуальную самооборону в случае вооруженного нападения. Но считать ли кибератаку вооруженным нападением? Статья 2 Устава говорит о воздержании от угроз силового воздействия на территориальную неприкосновенность или политическую независимость. Но можно ли считать пересечение нескольких сетевых пакетов из одного сегмента интернета в другой нарушением территориальной целостности? А должен ли рассматриваться взлом веб-сайта и размещение на нем призывов к свержению действующей власти как угроза политической независимости? Статьи 41 и 42 допускают применение невооруженных мер воздействия на нарушителей решений Совета Безопасности, но среди них не упоминается киберпространство — все ограничивается воздушным и морским пространствами, а также сушей.

39-я статья Устава ООН постулирует мысль, что Совет Безопасности ООН определяет угрозы миру. Но за все время своего существования он так и не опреде-

лился с тем, что такое киберугрозы. Попытки одного из постоянных членов Совета Безопасности (речь идет о России) инициировать эту работу также не увенчались успехом. Правила поведения в области обеспечения международной информационной безопасности, подготовленные странами ШОС и продвигаемые на уровне ООН, пока не приняты. Отдельные члены ООН препятствуют этим усилиям. Альтернативы в мире нет. Правоприменительной практики тоже. Видимо, именно поэтому авторы Таллинского руководства пытаются найти обоснование для применения уже существующих международных норм к киберпространству. Ведь надежд на выработку всеобщих правил немного, а угроза становится все реальней.

В КАЧЕСТВЕ ЗАКЛЮЧЕНИЯ

Атрибуция киберугроз — достаточно непростая задача, которая отличается от аналогичной в мире физическом тем, что, во-первых, мы не в состоянии идентифицировать нарушителя и установить его мотивацию только техническими методами. А во-вторых, спецоперации в киберпространстве часто реализуются сразу в нескольких юрисдикциях, а это требует взаимодействия и сотрудничества, не всегда возможного в текущей геополитической ситуации, когда отдельные государства не доверяют друг другу.

В таком небольшом материале достаточно сложно рассказать обо всех особенностях атрибуции киберугроз. Мы видим, что существуют объективные и субъективные сложности в правильном определении источника операций в киберпространстве. Мы понимаем, что в текущей геополитической ситуации очень часто тому или иному государству выгодно заявлять об атаках со стороны другого государства, даже не предъявляя серьезных доказательств. Мы понимаем, что существуют различные методы, позволяющие хотя бы определиться со страной, которая является источником киберугроз, но… К сожалению, пока у нас нет (исключая, быть может, оперативную разработку) методов, позволяющих провести четкую грань между атакой со стороны частного, негосударственного актора и нападением, за которым стоит держава, а значит, тема атрибуции киберугроз не закрыта и будет продолжена.

Примечания

1 Таллинское руководство — https://ccdcoe.org/research.html

2 Stuxnet — https://en.wikipedia.org/wiki/Stuxnet

3 FireEye — https://www.fireeye.com/current-threats/threat-intelligence-reports.html

4 Cylance — http://cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf

5 Маска — https://securelist.com/blog/research/58254/the-caretomask-apt-frequently-asked-questions/

6 Group-IB — http://www.group-ib.ru/index.php/7-novosti/1929-bolee-600-rossijskikh-internet-resursov-byli-atakovany-khakerami-terroristicheskoj-organizatsii-islamskoe-gosudarstvo-iraka-i-levanta

7 Taia — http://taia.global/wp-content/uploads/2015/02/SPE-Russia-Connection_Final.pdf

8 Snake — http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper.pdf

9 Ababil — http://tools.cisco.com/security/center/viewAlert.x?alertId=30207

10 Moonlight Maze — https://www.academia.edu/6182336/MOONLIGHT_MAZE._The_beginning_of_a_new_era

11 Взлом Twitter Assoaciated Press (стр. 23) — http://www.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/

12 Q-модель — http://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382

13 Атака на KHNP — http://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack