Великий и ужасный Huawei

12 марта 2018 года президент США Дональд Трамп заблокировал крупнейшее в истории слияние технологических компаний, не позволив сингапурскому чипмейкеру Broadcom купить за 117 миллиардов долларов компанию Qualcomm, ведущего разработчика микропроцессоров и модемов для мобильных телефонов. Свое решение американский лидер объяснил тем, что Broadcom может предпринять действия, способные поставить под угрозу национальную безопасность США.

Вето американского президента охладило пыл даже такого энтузиаста M&A-сделок [mergers and acquisitions, слияние и поглощение], каким считается гендиректор Broadcom Хок Тан, и слияние расстроилось.

Казалось бы, о какой угрозе безопасности идет речь? Тан имеет гражданство и проживает в США, большая часть штата Broadcom работает в этой стране, гарантами сделки готовы были выступить американские инвестиционные фонды, плюс в рамках слияния Broadcom обещала перенести штаб-квартиру из Сингапура назад в Калифорнию.

Однако практически сразу выяснилось, что запрет сделки напрямую связан ни с кем иным, как с Huawei, сообщает Bloomberg.

Благодаря госконтрактам и практически неограниченным кредитам Huawei стала одним из национальных чемпионов КНР. Это крупнейшая технологическая компания Поднебесной, объем выручки которой на 60 процентов превышает оборот китайского гиганта электронной коммерции JD.com.

Имея штат в 180 тысяч человек, большинство из которых инженеры, Huawei продает свою продукцию в 170 странах мира. Не являясь публичной компанией, Huawei, тем не менее, дважды в год публикует финансовые отчеты, чтобы убедить иностранных партнеров заключать с ней контракты. По данным Huawei, ее выручка в 2017 году достигла 92 миллиардов долларов, тогда как еще пять лет назад продажи были на уровне 35 миллиардов долларов. В 2018 году компания рассчитывает зарегистрировать уже 12-значный показатель.

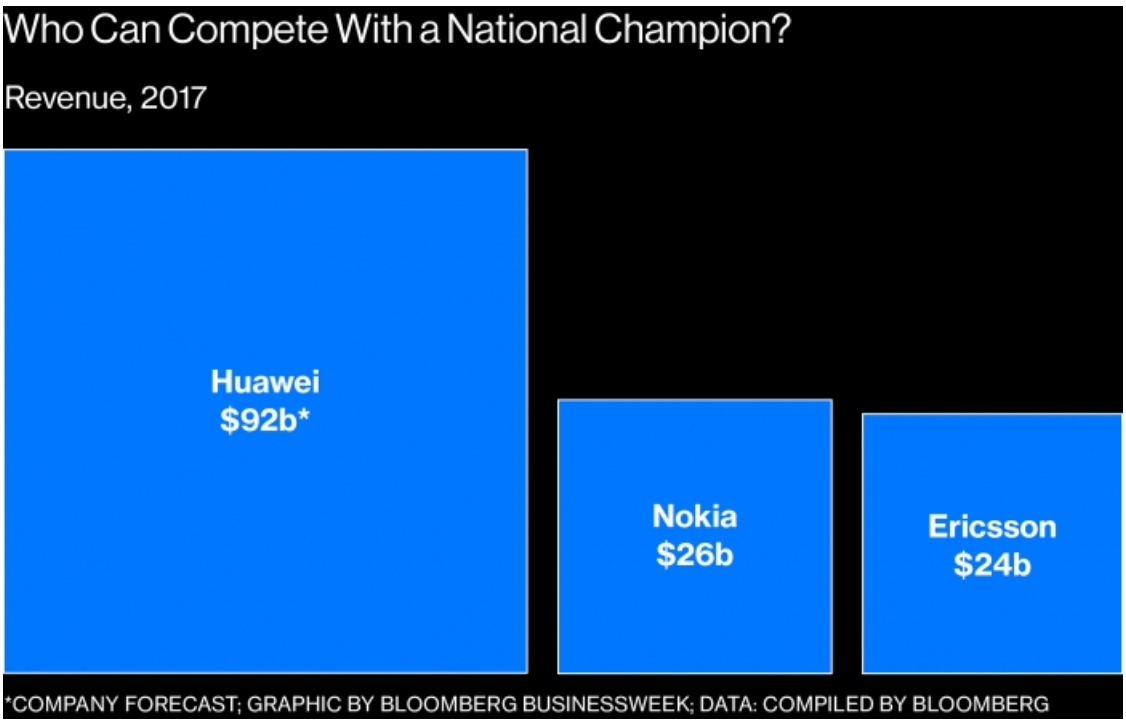

График с выручкой Huawei, Nokia и Ericsson за 2017 год

Несмотря на то, что "большой четверке" американских операторов - AT&T, Verizon, T-Mobile и Sprint - фактически запрещено пользоваться техникой китайского вендора, Huawei остается одним из лидеров в области телекоммуникационного и сетевого оборудования. Кроме того, компания уверенно наращивает присутствие на мировом рынке смартфонов: по итогам 2017 года доля Huawei составила 10,4процента против 9,5 процента годом ранее (данные IDC).

Huawei - третий по величине производитель смартфонов, не только опережает по темпам роста лидеров отрасли Samsung и Apple, но уже обладает достаточными производственными мощностями и технологическими ноу-хау, чтобы конкурировать с Qualcomm в гонке за лидерство в области 5G-технологий, которые должны приблизить эру беспилотного транспорта, сделать возможным дистанционное управление медицинскими устройствами и промышленным оборудованием.

У Huawei множество возможностей для роста, особенно если компания займет сильные позиции в разработке стандартов 5G. К настоящему времени Huawei зарегистрировала примерно 10% от общего числа патентов в области 5G, и в компании говорят, что ее лучшие инженеры продолжают работу на этом направлении.

Потратив уже около 600 миллионов долларов на 5G-исследования, Huawei планирует в 2018 году выделить еще 800 миллионов долларов на то, чтобы вывести технологию на рынок. Компания уже заключила около 50 контрактов с мобильными операторами на тестирование своего оборудования. В 2016 году Huawei потратила на НИОКР порядка 12 миллиардов долларов, тогда как американская Qualcomm и финская Nokia направили на эти цели 5,1 и 4,9 миллиарда долларов соответственно.

Получив преимущество на рынке 5G-технологий, Huawei сможет "выкачивать" миллиарды из своих конкурентов в США и других стран, обложив их лицензионными сборами за право пользования своими патентами в этой сфере. Усиливающееся влияние и перспектива попасть в зависимость от китайского ИТ-гиганта пугает американских политиков, но еще больше их повергает в ужас то, что власти КНР могут воспользоваться тайными лазейками в сетевом оборудовании Huawei, чтобы шпионить за жителями США, их телефонными звонками, смс-сообщениями и электронной перепиской.

Как со всем этим связана несостоявшаяся сделка Broadcom? В Белом доме посчитали, что купив Qualcomm, Broadcom захочет ограничить ее расходы на исследования и разработки, что косвенно даст Huawei еще больше преимуществ в разработке стандартов и оборудования для 5G-сетей.

Перед этим отрицательную оценку сделке дали в Комитете по иностранным инвестициям в США (CFIUS, Committee on Foreign Investment in the United States). В ведомстве заявили, что поглощение подорвало бы позиции Qualcomm и открыло бы Huawei дорогу к расширению влияния в сфере 5G-технологий. В Комитете напомнили о существующих опасениях в отношении Huawei и других ее соотечественниц и подчеркнули, что доминирование Китая может обернуться серьезными негативными последствиями для национальной безопасности Соединенных Штатов.

Противодействие вендорам из Поднебесной в США усиливается. В январе 2018 года конгрессмен-республиканец Майк Конэвей предложил законопроект, который запретит федеральному правительству США сотрудничать с фирмами, использующими оборудование производства Huawei и ZTE. Причиной ограничений указывалась тесная связь компаний с китайским правительством и возможность шпионажа с их стороны.

Двумя неделями позднее в прессу просочились документы Совета национальной безопасности США (National Security Council, NSC), в которых говорилось о развитии 5G сетей в стране, а прогресс китайских технологических компаний в этой сфере назывался прямой угрозой безопасности американцев. В проекте NSC предлагалось в ближайшие три года создать единую централизованную сеть 5G по всей стране и как вариант рассматривалась возможность ее строительства за счет государственных денег, то есть национализации, с целью защититься от проникновения Китая.

Еще через пару недель, выступая в комитете по разведке Сената США (Senate Intelligence Committee), главы шести ведущих разведывательных служб, включая ЦРУ, ФБР и АНБ, посоветовали американцам не пользоваться продуктами и сервисами китайских производителей.

Все эти усилия не прошли даром. Под нажимом властей американские операторы AT&T и Verizon отказались от планов по продаже смартфонов Huawei в своих магазинах, а недавно СМИ сообщили о том, что в ближайшие недели реализацию устройств китайского вендора прекратит еще и крупнейший ритейлер Best Buy.

Между тем, в Huawei отвергают все подозрения и в ответ обвиняют США в национализме и шпиономании. В компании заверяют, что они связаны с китайским правительством не более чем Apple или Google, и что закладка лазеек (бэкдоров) для шпионажа в сетевом оборудовании или программном обеспечении равносильна самоубийству на рынке.

> "Мы уже 30 лет в этом бизнесе, и не было ни единого киберинцидента. Разве Америке нужно опасаться нас в плане кибербезопасности? Ответ – однозначно нет", - заявил вице-президент Huawei по взаимодействию с зарубежными СМИ Джо Келли.

В правительстве Китая осуждают действия американских властей и говорят, что прикрываясь защитой национальной безопасности, США ведут политику торгового протекционизма. Официальное издание Коммунистической партии Китая "Жэньминь жибао" в своем аккаунте Weibo (китайский аналог Twitter) в феврале 2018 года писало, что стремительный подъем Huawei и уверенное укрепление Китая и ее интернет-компаний заставляет США нервничать. Позднее пост был удален.

Несмотря на ограничительные меры США, большинство других стран, в том числе союзники Соединенных Штатов, продолжают использовать продукты Huawei в своей сетевой инфраструктуре, но тщательно поверяют оборудование на наличие возможных уязвимостей. Так, в рамках соглашения с Великобританией в 2010 году в английском городе Банбери был открыт центр Huawei Cyber Security Evaluation Centre (HCSEC), также известный как Cell. В организации, созданной для оценки возможных киберрисков, связанных с использованием оборудования Huawei, работают сотрудники китайского вендора, а офицеры британских разведслужб контролируют их и анализируют программный код Huawei на предмет бэкдоров. Отсутствие претензий к центру в Huawei использовали как PR-ход для дальнейшего расширения своей деятельности в Западной Европе.

Однако в США такие доводы считают неубедительными, мотивируя тем, что лазейки в системе безопасности очень трудно найти, если только не знать, где именно искать. В ПО современных коммутаторов для беспроводных сетей миллионы строчек программного кода, и оборудование может быть скомпрометировано на разных этапах производства или во время одного из регулярных обновлений системы.

Как показал скандал с уязвимостями Spectre и Meltdown в процессорах Intel, подобные аппаратные бреши могут годами оставаться незамеченными и их практически невозможно предвидеть или обнаружить. В самых кошмарных сценариях американских спецслужб Huawei внедряет бэкдор на уровне чипов, затем дистанционно активирует его и нажатием пары клавиш открывает всю сеть китайским военным.

Американские политики опасаются такого развития событий отчасти потому, что разведслужбы США сами запросто используют свои отечественные компании ровно для того же. AT&T, один из крупнейших американских операторов, так охотно помогал Агентству национальной безопасности США с прослушкой, что даже получил от АНБ благодарность за готовность к содействию, о чем выяснилось из материалов, переданных в 2013 году журналистам "Нью-Йорк Таймс" экс-сотрудником АНБ Эдвардом Сноуденом. Из них же стало известно, что американские спецслужбы внедряли жучки в устройства американских и азиатских производителей, включая Cisco, Huawei и Juniper, а также использовали уязвимости в оборудовании Huawei для шпионажа.

> "Ирония в том, они делают с нами как раз то, в чем всегда обвиняли Китай", - заявил тогда по поводу вскрывшейся информации представитель Huawei.