

УДК 327

Карина ГЕМУЕВА

HUAWEI В СТРАНАХ ЕС: ПРОБЛЕМА УЧАСТИЯ В РАЗВИТИИ СЕТЕЙ 5G

Аннотация. Статья посвящена анализу мотивов различных акторов, как в рамках ЕС, так и внешних игроков, по вопросу участия Huawei в развитии сетей 5G в странах Евросоюза. Подчёркивается сложность баланса интересов всех заинтересованных сторон и учёта возможных негативных последствий политическими элитами стран ЕС. Выделен ряд факторов, проявившихся во время борьбы с пандемией коронавируса, которые могут повлиять на будущие решения стран ЕС. Поставлен вопрос о возможности конструктивного диалога на болезненные темы, включая рассматриваемый вопрос, в условиях ведения информационных войн. Высказывается предположение, что крупные страны ЕС последуют по пути «компромиссных решений», максимально снижая возможные риски безопасности и вместе с тем не исключая Huawei из числа возможных поставщиков.

Ключевые слова: сети 5G, телекоммуникационные сети, Huawei, ЕС, Китай, США.

Наличие современной телекоммуникационной инфраструктуры является необходимым условием для цифровизации экономики Евросоюза. Доминирующее положение среди поставщиков телекоммуникационных решений на рынке ЕС занимают европейские компании *Nokia*, *Ericsson* и китайская компания *Huawei*. В условиях непосредственной вовлечённости последней в экономический конфликт между Китаем и США в странах ЕС разгораятся дискуссии относительно участия *Huawei* в развитии сетей 5G.

Интересы и мотивы различных акторов внутри стран ЕС

В рамках отдельных стран ЕС вариативность интересов сторон определяется типом акторов и преваляцией экономических или политических мотивов, либо же вопросов безопасности. Например, операторы мобильных сетей прежде всего руководствуются коммерческими интересами. По оценке международной ассоциации *GSMA*, введение полного запрета на участие китайских компаний *Huawei* и *ZTE* в развёртывании сетей 5G в Европе обернётся дополнительными затратами в размере 62 млрд долл. и задержкой на 18 месяцев коммерциализации сетей пятого поколения¹. В отчёте *Strand Consult* даётся более консервативная оценка затрат на сумму 3,5 млрд долл.² Расходы операторов будут сильно варьироваться в зависимости от строгости запрета и масштабов использования оборудования *Huawei* в действующих сетях 4G. Поскольку принятие адресных мер к китайской компании носило бы дискримина-

© Гемуева Карина Алиевна – младший научный сотрудник, Центр европейских исследований ИМЭМО им. Е.М. Примакова РАН. Адрес: 117997, Россия, Москва, ул. Профсоюзная д. 23. E-mail: Krina07@mail.ru.

Статья поступила в редакцию: 22.05.2020.

DOI: <http://dx.doi.org/10.15211/vestnikieran320207581>.

¹ Europe's 5G to cost \$62 billion more if Chinese vendors banned: telcos. 07.06.2019. URL: <https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3> (дата обращения: 21.05.2020).

² Strand Consult. The real cost to rip and replace of Chinese equipment in telecom networks. 09.2019. URL: <https://d110erj175o600.cloudfront.net/wp-content/uploads/2019/10/Strand-Consult-The-real-cost-to-rip-and-replace-of-Chinese-equipment-in-telecom-networks-003-1.pdf> (дата обращения: 21.05.2020).

ционный характер, ЕС идёт по пути повышения требований к безопасности сетей и защите личных данных потребителей для всех участников рынка, что также подразумевает дополнительную финансовую нагрузку на сектор.

Национальные агентства по кибербезопасности и спецслужбы при оценке деятельности *Huawei* закономерно отдают приоритет вопросам безопасности. Например, в декабре 2018 г. в отчёте Национального управления по кибернетической и информационной безопасности Чехии (NCISA) было указано, что использование оборудования и программных компонентов китайских компаний *Huawei* и *ZTE* представляет угрозу безопасности страны¹. Вместе с тем Бельгийский центр кибербезопасности (ССВ) объявил, что не обнаружил достаточных доказательств для установления какой-либо угрозы со стороны *Huawei* вопреки выдвинутым в США обвинениям *Huawei* в шпионаже в пользу властей КНР².

Позиции различных ведомств варьируются в зависимости от того, оцениваются ли фактические действия, представляющие угрозу, или же потенциальные риски. Во втором случае зачастую выдвигаются такие доводы, как агрессивная деятельность китайских спецслужб на территории конкретных стран ЕС, предположительно тесные связи *Huawei* с правительством КНР и военными структурами, и не в последнюю очередь – трактовка положений Закона о национальной безопасности КНР об обязательствах, находящихся на территории Китая компаний, «оказывать помощь в работе, связанной с государственной безопасностью». Именно этот пункт закона вызвал сильную реакцию в зарубежных странах и породил подозрения в использовании Китаем национальных телекоммуникационных компаний для шпионажа. Однако представители *Huawei* утверждают, что положения Закона не требуют от компаний действий, противоречащих законодательству других стран, и не дают право китайскому правительству требовать от производителей внедрения бэкдоров в своё оборудование³.

В свою очередь сама компания *Huawei* также является непосредственным участником дискуссии. По мере эскалации конфликта компания кардинально поменяла свою «внешнюю политику», активно вступая в диалог, выдвигая контраргументы и доводы в свою пользу и придавая большее значение развитию связей с общественностью. В ответ на озвучиваемые в странах ЕС опасения компания в ноябре 2018 г. открыла центр кибербезопасности в Бонне (Германия), а в марте 2019 г. – центр кибербезопасности и прозрачности в Брюсселе, где клиенты и регулирующие органы могут проводить тестирование оборудования и программных компонентов *Huawei*, включая проверку исходного кода.

Стоит отметить демонстрируемую готовность *Huawei* открыть в странах ЕС производственные мощности, ориентированные непосредственно на европейский рынок. Так, в феврале 2020 г. компания заявила о плане строительства завода во Франции. Весомыми аргументами в таких предложениях служат повышение занятости и планируемый объём вложений. Для *Huawei* это прежде всего политический шаг, призванный укрепить доверие к компании, поскольку с коммерческой точки зрения открывать производственные мощности в странах Западной Европы не выгодно вследствие более высоких издержек.

¹ National Cyber and Information Security Agency. Warning. 17.12.2018. URL: <https://www.govcert.cz/download/kii-vis/Warning.pdf> (дата обращения: 21.05.2020).

² Huawei: No proof of spying in Belgium says Cyber-security Centre. 15.04.2019. URL: <https://www.brusselstimes.com/all-news/belgium-all-news/politics/55488/huawei-no-proof-of-spying-in-belgium-says-cybersecurity-centre/> (дата обращения: 21.05.2020).

³ Huawei admit Chinese law obliges companies to work with government, under conditions. 11.04.2019. URL: <https://www.euractiv.com/section/cybersecurity/news/huawei-admit-chinese-law-obliges-companies-to-work-with-government/> (дата обращения: 21.05.2020).

Внешнее влияние на страны ЕС: Китай и США

В условиях торговой войны между Китаем и США обе стороны конфликта оказывали давление на страны ЕС, вплоть до явных и неявных угроз, относительно участия *Huawei* в развитии сетей 5G в Европе. Действия США включали призывы к должностным лицам исключить использование оборудования *Huawei*, исходя из рисков информационной безопасности, и активную пропаганду своей позиции в СМИ и в среде экспертного сообщества. Наибольшему воздействию подверглись союзники США по НАТО: высказывались предостережения, что опора на китайских поставщиков может поставить под угрозу разведывательные и коммуникационные возможности и, соответственно, сотрудничество в рамках альянса.

Послы Китая в странах ЕС также предупреждали о последствиях, преимущественно экономического характера, с которыми могут столкнуться страны, исключившие *Huawei* из списка возможных поставщиков и подрядчиков по внеэкономическим соображениям. Вмешательство правительства КНР, с одной стороны, может быть оправдано защитой интересов национального бизнеса, противодействию американским шагам по дискредитации и сдерживанию китайских компаний-лидеров в сфере высоких технологий, но, с другой стороны, предоставляет оппонентам дополнительные аргументы относительно тесных связей этой частной компании с государством. Примером могут служить слова У. Кена, посла КНР в Германии, о возможных последствиях для Германии в случае исключения *Huawei* с рынка телекоммуникаций. В том же заявлении была подчёркнута важность китайского рынка для немецких автопроизводителей¹. В ряде случаев официальных заявлений со стороны Китая даже не требовалось, поскольку многие политические лидеры стран ЕС «превентивно» учитывают вероятность и последствия ответных мер КНР в случае принятия соответствующих решений.

Страны, сильно тяготеющие к одному из двух полюсов силы, заняли вполне ожидаемые позиции. Например, Венгрия, как важный политический партнер Китая в ЕС, «не видит доказательств, что оборудование *Huawei* может представлять угрозу безопасности» и планирует привлечь *Huawei* к развёртыванию сетей 5G². С другой стороны, Польша, Румыния и Эстония подписали меморандумы с правительством США о безопасности в сетях мобильной связи 5G. Хотя это и нельзя считать окончательным решением, но демонстрирует вполне однозначную позицию.

Однако для большинства стран ЕС, стремящихся развивать сотрудничество как с Китаем, так и с США, вопрос выбора определённой позиции представляется намного более сложным.

Во-первых, отсутствие достоверной первичной информации и независимой авторитетной экспертной оценки не позволяет ряду акторов, в том числе не обладающим необходимыми компетенциями в сфере кибербезопасности малым странам ЕС, принять аргументированное решение по рассматриваемому вопросу.

Во-вторых, конфликт интересов бизнеса и агентств национальной безопасности, поляризация мнений среди политической элиты затрудняет формулирование чёткой единой позиции, исходя из национальных интересов членов ЕС. К причинам промедления с вынесением окончательного решения можно отнести и нежелание политических лидеров принять ответственность за возможные негативные последствия экономического, социального и политиче-

¹ Chinese ambassador accused of threatening German car industry if Huawei is frozen out. 15.12.2019. URL: <https://www.scmp.com/news/china/diplomacy/article/3042190/chinese-ambassador-accused-threatening-german-car-industry-if> (дата обращения: 21.05.2020).

² Hungarian minister opens door to Huawei for 5G network rollout. 05.11.2019. URL: <https://www.reuters.com/article/us-hungary-telecoms-huawei/hungarian-minister-opens-door-to-huawei-for-5g-network-rollout-idUSKBN1XF12U> (дата обращения: 21.05.2020).

ского характера.

В-третьих, формулирование единой стратегии по данному вопросу на уровне Евросоюза требует консенсуса всех стран-участниц, что с учётом диаметрально противоположных позиций ряда стран приводит к принятию «компромиссного» варианта и не позволяет объединению проводить единую жёсткую политику. Так, в январе 2020 г. был опубликован комплекс мер, направленных на снижение рисков безопасности при развитии сетей 5G (EU Toolbox). Это стало третьим шагом после национальной оценки риска и факторов уязвимости сетей 5G странами-участницами и последующей публикации скоординированной оценки риска на уровне ЕС в рамках формирования согласованного подхода к безопасности сетей 5G, рекомендованного Еврокомиссией в марте 2019 г. Данный комплекс мер не вводит явного запрета на участие *Huawei* в развитии сетей 5G в странах ЕС, однако подчёркивается необходимость снизить зависимость от конкретных поставщиков и ограничить использование оборудования «поставщиков с высоким риском» в базовых сетях. Тем не менее, допускается широкое толкование «поставщиков с высоким риском» различными странами-участницами и не ограничивается вариативность будущих решений.

В таких условиях члены ЕС фактически оказываются один на один с акторами, несопоставимыми с ними по экономическому и политическому весу, что открывает главным участникам торгового конфликта возможность для массивного продвижения собственных интересов. Более того, при отсутствии единой независимой стратегии, направленной на защиту интересов объединения, позиции ЕС как глобального игрока на рынке ИКТ могут быть ослаблены и утрачен инновационный потенциал, необходимый для удержания конкурентных преимуществ при переходе к новому технологическому укладу.

Влияние коронавируса на деловые связи Китая и стран ЕС

Казалось бы, на время общемировой борьбы с коронавирусом логичным решением будет заключить «временное перемирие», тем более что ключевые решения по данным вопросам откладываются на неопределённые сроки. Так, ряд государств ЕС перенесли проведение аукционов на частоты 5G, запланированных на первые месяцы 2020 г. Однако мы наблюдаем обратную картину: связанная с пандемией коронавируса тематика, вызывающая острую, а подчас иррациональную реакцию всех слоёв общества, становится дополнительным инструментом психологического воздействия в информационной войне на население стран ЕС.

При анализе действий различных акторов во время общемировой борьбы с коронавирусом интерес представляет не столько оценка конкретных мер и отделение фактов от голословных обвинений, сколько характер деятельности, реакция других игроков и возможные последствия, в том числе для участия *Huawei* в развёртывании сетей 5G на территории ЕС.

Прежде всего, необходимо упомянуть разногласия относительно благотворительных поставок китайских компаний, в том числе *Huawei*, медицинского оборудования и средств индивидуальной защиты в страны ЕС для борьбы с коронавирусом. «Спусковым крючком» послужило высказывание Ж. Борреля, верховного представителя ЕС по иностранным делам и политике безопасности, об «идушей битве нарративов», «попытках дискредитировать ЕС» со стороны Китая, геополитических интересах, стоящих за проведением «политики щедрости»¹. Последующее заявление Т. Бретона, комиссара ЕК по вопросам внутреннего рынка, что он не видит никаких скрытых мотивов в предоставлении компанией *Huawei* защитных масок стра-

¹ EU HRVP Josep Borrell: The Coronavirus pandemic and the new world it is creating. 24.03.2020. URL: https://eeas.europa.eu/delegations/china/76401/eu-hrvp-josep-borrell-coronavirus-pandemic-and-new-world-it-creating_en (дата обращения: 21.05.2020).

нам ЕС¹, в очередной раз демонстрирует отсутствие чёткой единой позиции на уровне ЕС. Политизация ситуации и резко негативная реакция со стороны различных акторов побудили *Huawei* свернуть благотворительную программу поставок медицинских масок в Европу.

Другим поводом для дискуссий послужило такое новое явление во внешней политике КНР, обычно отличающейся взвешенным подходом и осторожностью оценочных суждений, как агрессивная пропаганда своей позиции с использованием инструментов публичной дипломатии. В общих чертах подобные методы являются своего рода «визитной карточкой» американской внешнеполитической практики в XXI в., включая твиттер-дипломатию, применение дезинформации и необоснованных обвинений в адрес оппонента, психологических методов воздействия на общественное мнение для создания благоприятного информационного поля. Основными «проводниками» агрессивной линии Пекина стали представители новой волны китайских дипломатов, которых в западных СМИ окрестили «волками-воинами» по аналогии с персонажами китайского художественного фильма 2017 г. «Война волков».

Конкретным примером использования новых методов публичной дипломатии в странах ЕС стала публикация на сайте посольства КНР во Франции, содержащая критические замечания о деятельности французских властей по борьбе с коронавирусом, в том числе обвинения в том, что французы намеренно оставили своих пожилых жителей умирать в домах престарелых².

В целом в большинстве заявлений «волков-воинов» акцентировались промахи местных властей в условиях демократических режимов стран Запада, что противопоставлялось эффективным методам Коммунистической партии Китая по борьбе с вирусом³. Ответной реакцией в странах ЕС стала беспрецедентная волна критики, невзирая на фактическую гуманитарную помощь и даже в ряде случаев зависимость от поставок медикаментов и медицинского оборудования из Китая.

В некоторых европейских странах власти КНР обвинялись в сознательном занижении данных официальной статистики по числу заболеваний и смертей от коронавируса. Впрочем, суждения европейских политиков всё же далеки от радикальных высказываний официальных лиц США, включая требования к Китаю взять на себя ответственность за распространение коронавируса по всему миру, вплоть до выплат компенсаций за каждого погибшего от вируса американца.

В какой степени перечисленные факторы отразятся на решениях ЕС по поводу участия *Huawei* в развёртывании сетей 5G пока неясно, однако можно заметить определённые тенденции к изменению позиций Брюсселя по сравнению с реалиями до начала пандемии коронавируса. Зависимость от внешних поставок, в особенности жизненно необходимого медицинского оборудования и средств индивидуальной защиты в кризисное время, подрывает доверие к базовым принципам международного разделения труда на основе конкурентных преимуществ отдельных регионов. Во многих странах наблюдается сворачивание курса на углубление глобализации, акцентируются меры по переносу или организации производств критически важных товаров на своей территории. Агрессивный характер публичной дипломатии Китая также вызывает серьёзную обеспокоенность со стороны политических элит стран ЕС. На этом

¹ EU industry chief sees no quid pro quo in Huawei's «mask diplomacy». 01.04.2020. URL: <https://www.reuters.com/article/health-coronavirus-eu-huawei-tech/corrected-eu-industry-chief-sees-no-quid-pro-quo-in-huaweis-mask-diplomacy-idUSL8N2BO7RD> (дата обращения: 21.05.2020).

² Joseph de Weck. China's COVID-19 Diplomacy is Backfiring in Europe. 21.04.2020. URL: <https://www.fpri.org/article/2020/04/chinas-covid-19-diplomacy-is-backfiring-in-europe/>

³ Small A. The meaning of systemic rivalry: Europe and China beyond the pandemic. 13.05.2020. URL: <https://www.ecfr.eu/publications/summary/the-meaning-of-systemic-rivalry-europe-and-china-beyond-the-pandemic> (дата обращения: 21.05.2020).

фоне существующие противоречия в двусторонних отношениях, включая нарушения прав интеллектуальной собственности китайскими компаниями и демпинг с их стороны¹, могут привести к частичному или кардинальному пересмотру характера взаимоотношений с Китаем.

Дискуссии вокруг *Huawei* как пример коммуникации на международном уровне

Глобальной тенденцией нового времени является взаимопроникновение и взаимовлияние различных аспектов жизни общества, расширение круга вовлечённых во внешнеполитическую деятельность акторов, изменение механизмов взаимодействия. Ряд изначально национальных проблем переходит в разряд глобальных феноменов, которые требуют конвергенции, объединения и консолидации всего мирового сообщества². Необходимость учёта позиций различных акторов, баланса интересов в экономической, политической, социальной и прочих сферах многократно усложняет формулирование и реализацию независимой долгосрочной стратегии развития, исходя из национальных интересов.

Случай с компанией *Huawei* служит наглядным примером того, как предположения о наличии рисков информационной безопасности могут привести к ожесточённым политическим дебатам, хотя первоначально вопросы выбора определённого подрядчика носили скорее технический и экономический характер. Сомнения в истинности аргументов обеих сторон конфликта искусственно подогреваются регулярным вбросом новой непроверенной информации в СМИ. Гипотетическая угроза общественной безопасности вызывает крайне острую реакцию всех слоёв общества. Политические деятели и даже технические специалисты напрямую или косвенно могут служить проводниками интересов посторонних акторов. В данной ситуации становится сложным отделить факты от суждений, экспертную оценку от навязываемого мнения. Рассматривая данную проблему в контексте меняющихся на глазах принципов международных отношений, включая ведущиеся информационные войны, правомерно задать вопросом, насколько в принципе реален продуктивный и конструктивный диалог на болезненные темы в существующих условиях.

* * *

Затянувшиеся дискуссии по поводу участия китайской компании *Huawei* в развёртывании сетей 5G на территории ЕС вскрывают ряд глубинных противоречий. Во-первых, наблюдается конфликт интересов различных акторов на уровне стран-участниц, в том числе операторов мобильных сетей, национальных агентств по кибербезопасности и спецслужб, а также самой компании *Huawei*. Во-вторых, страны ЕС оказались вовлечены в экономический конфликт между Китаем и США и испытывают давление с обеих сторон. В-третьих, можно выделить ряд факторов, проявившихся во время борьбы с пандемией коронавируса, которые могут изменить баланс сил в будущем. В связи с этим политические элиты стран ЕС поставлены перед сложной задачей: соблюдать баланс интересов акторов на внутреннем рынке, вносить коррективы в формат взаимодействия между ЕС и Китаем, исходя из своих долгосрочных стратегических интересов, учитывать реакцию внешних игроков и её возможные негативные последствия экономического, социального и политического характера. Можно предположить, что крупные страны ЕС последуют по пути «компромиссных решений», максимально снижая потенциальные риски безопасности и вместе с тем не исключая *Huawei* из числа возможных

¹ Носов М.Г. ЕС-Китай: эпидемия коронавируса может помешать завершению переговоров об инвестиционном соглашении. Европейский Союз: факты и комментарии, №99, 2020. С. 120-123. DOI: <http://dx.doi.org/101521/eufacts12020120123>.

² Морозова Н.И., Бурякова О.С., Алиева Н.З. Конвергенция информационной безопасности в цифровом пространстве: нелинейный аспект. Фундаментальная и прикладная наука: состояние и тенденции развития, 2020. С. 201.

поставщиков. Много будет зависеть от характера диалога с заинтересованными сторонами, осложнённого кризисом эффективной коммуникации на международном уровне вследствие ведущихся информационных войн.

Список литературы

Морозова Н.И., Бурякова О.С., Алиева Н.З. Конвергенция информационной безопасности в цифровом пространстве: нелинейный аспект. *Фундаментальная и прикладная наука: состояние и тенденции развития*, 2020. С. 200-204.

Носов М.Г. ЕС–Китай: эпидемия коронавируса может помешать завершению переговоров об инвестиционном соглашении. *Европейский Союз: факты и комментарии*, №99, 2020. С. 120-123. DOI: <http://dx.doi.org/101521/eufacts12020120123>.

References

Morozova N.I., Buryakova O.S., Alieva N.Z. Konvergenciya informacionnoj bezopasnosti v cifrovom prostranstve: nelinejnyj aspekt. *Fundamental'naya i prikladnaya nauka: sostoyanie i tendencii razvitiya*, 2020. С. 200-204.

National Cyber and Information Security Agency. 2018. Warning. URL: <https://www.govcert.cz/download/kii-vis/Warning.pdf> (дата обращения: 21.05.2020).

Nosov M.G. ES-Kitaj: epidemiya koronavirusa mozhet pomeshat' zaversheniyu peregovorov ob investicionnom soglashenii. *Evropejskij Soyuz: fakty i kommentarii*, №99. 2020. P. 120-123. DOI: <http://dx.doi.org/101521/eufacts12020120123>.

Small A. The meaning of systemic rivalry: Europe and China beyond the pandemic. 2020. URL: https://www.ecfr.eu/publications/summary/the_meaning_of_systemic_rivalry_europe_and_china_beyond_the_pandemic (дата обращения: 21.05.2020).

Strand Consult. The real cost to rip and replace of Chinese equipment in telecom networks. 09.2019. URL: <https://d110erj175o600.cloudfront.net/wp-content/uploads/2019/10/Strand-Consult-The-real-cost-to-rip-and-replace-of-Chinese-equipment-in-telecom-networks-003-1.pdf> (дата обращения: 21.05.2020).

Huawei in EU Countries: Participation in the Development of 5G Networks

Author. Karina Gemueva, Junior researcher, IMEMO RAS. **Address:** 23, Profsoyuznaya str., Moscow, Russia, 117997. **E-mail:** krina07@mail.ru.

Abstract. The article is dedicated to the analysis of the varied motivations of both internal and external players involved, regarding the involvement of Huawei in the 5G network deployment in the EU. The author emphasizes a complexity of balancing the interests of all stakeholders and considering possible negative consequences by the political elites in EU countries. A number of factors emerged during the fight against the coronavirus pandemic, which may affect future decisions of the EU countries, are highlighted. The author raises a question about the possibility of a constructive dialogue on sensitive topics, including the issue under consideration, in the context of ongoing information warfare. It is suggested that large EU countries will follow the path of «compromise solutions», minimizing possible security risks and at the same time not excluding Huawei from the list of possible suppliers.

Key words: 5G networks, telecommunication networks, Huawei, EU, China, USA.

DOI: <http://dx.doi.org/10.15211/vestnikieran320207581>.

Научно-аналитический вестник ИЕ РАН, 2020, №3