Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Маттиас Клаус, *Connections QJ* 20, № 2 (2021): 21-31
https://doi.org/10.11610/Connections.rus.20.2.03

Рецензированная статья

Доверие к провайдерам ИКТ: Помогут ли корпоративные меры кибердоверия?

Маттиас Клаус

Аннотация: Доверие в киберпространстве важно для укрепления безопасности, и оно ещё важнее, когда страны привлекают частные компании для разработки, строительства, обслуживания и функционирования своей информационно-коммуникационной инфраструктуры. В данной статье предлагается новый формат мер кибердоверия для достижения этой цели путём привлечения частного сектора, как равного партнёра. Страны могут использовать этот метод для проверки своих потенциальных поставщиков, чтобы снизить восприятие риска, а также установить и поддерживать доверительные отношения с ними.

Ключевые слова: доверие, безопасность цепочек поставок, киберриск, инфраструктура ИКТ, меры кибердоверия.

Вступление

Странам нужно либо доверять подрядчикам, либо запретить им строить и обслуживать инфраструктуру информационно-коммуникационных технологий (ИКТ). В мире, где технические знания и средства для разработки, эксплуатации и обслуживания инфраструктуры ИКТ почти всецело принадлежат частным компаниям, страны всё больше зависят от частного сектора. Поскольку защищённость поставляемого программного обеспечения и техники определить невозможно, доверие между клиентом и поставщиком имеет огромное значение, как и классическое доверие между гражданами, правительством и корпорациями.[1] Чтобы защитить свои интересы от угроз безопасности, страна выберет компанию, которой она доверяет. Она будет оценивать ИКТ провайдеров на основе доверия и прозрачности. Даже если

[1] George Cvetkovich and Ragnar E. Löfstedt, eds., *Social Trust and the Management of Risk* (London: Earthscan, 1999).

у страны нет заслуживающих доверия вариантов, ей всё равно нужно выбирать компанию. В Пражских предложениях 2019 г. (результаты международной конференции по безопасности 5G) это названо одним из самых важных политических рисков безопасности при управлении ИТ-инфраструктурой страны.[2] Эта задача критична и все более сложна, особенно учитывая, что один из главных кандидатов, Huawei, подозревают в контроле со стороны Компартии Китая (КПК).

Цель этой статьи — предложить меры укрепления доверия на основе уроков опыта работы с Huawei. Конкретно в ней предложена модель для не пользующихся доверием стран и компаний в виде скорректированных мер доверия для снижения риска потенциальных покупателей. Странам-покупателям это может дать гарантии при выборе подходящего ИКТ-провайдера, а поставщикам – возможность доказать свою прозрачность и независимость. В мире, где больше нет доверия, такое прозрачное и активное общение может помочь восстановить доверие и сохранить связь между участниками противоборствующих политических систем.[3]

Пример Huawei

Huawei – ведущая ИКТ-компания, которая поднялась за счёт крупных государственных субсидий и преференций на внутреннем рынке Китая.[4] Статус Huawei как «национального лидера» в такой высокотехнологичной отрасли, как ИКТ,[5] позволил ей стать крупнейшим в мире производителем телекоммуникационного оборудования и вторым производителем смартфонов.[6]

В Huawei утверждают, что это частная компания,[7] но её организация отличается от классической. Главный аргумент Huawei – то, что сотрудники компании одновременно являются её собственниками, почти 87 000 акционеров выбирают Представительскую комиссию. Комиссия избирает Совет

---

2 "The Prague Proposals: The Chairman Statement on Cyber Security of Communication Networks in a Globally Digitalized World," Prague 5G Security Conference, Prague, May 3, 2019, по состоянию на 12 марта 2020, https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf.

3 Ragnar E. Löfstedt, *Risk Management in Post-Trust Societies*, Earthscan Risk in Society series (London: Earthscan, 2008).

4 "The Real Cost to Rip and Replace of Chinese Equipment in Telecom Networks," *Strand Consult*, 2019, p. 12, по состоянию на 1 февраля 2020, https://strandconsult.dk/the-real-cost-to-rip-and-replace-chinese-equipment-from-telecom-networks.

5 Tai Ming Cheung, "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities," *Journal of Cyber Policy* 3, no. 3 (2018): 306-326, 311, https://doi.org/10.1080/23738871.2018.1556720.

6 Elsa Kania, "Much Ado about Huawei (part 1)," *The Strategist* (Australian Strategic Policy Institute), March 27, 2018, по состоянию на 9 марта 2020, https://www.aspistrategist.org.au/much-ado-huawei-part-1.

7 "Huawei's Position Paper on Cyber Security" (Huawei, November 2019), 61, по состоянию на 12 марта 2020, https://www-file.huawei.com/-/media/corp/facts/pdf/2019/huaweis-position-paper-on-cyber-security.pdf?la=en.

директоров и Наблюдательный совет, которые, в свою очередь, выбирают Правление.[8]

Хотя это отчасти верно, представительство компании умалчивает о важных деталях своих связей с КПК. Главное – 99% её акций принадлежат не основателю или сотрудникам, а профсоюзному комитету Huawei Investment & Holding. Профком Huawei Investment & Holding в конечном счёте подотчётен Всекитайской федерации профсоюзов, глава которой – член Политбюро ЦК Коммунистической партии Китая (КПК).[9] Следует также учитывать роль КПК в компании, о чём свидетельствует то, что её нынешний начальник отдела контроля и этики – партийный секретарь.

Китайские государственные банки тоже относятся к Huawei, как к государственной компании. Так, главный финансист Huawei – Китайский банк развития, который контролируется китайским правительством и является крупнейшим в мире кредитором.[10] Профиль рисков 2018 г. показывает, что Huawei получил миллиарды долларов финансирования и от нескольких государственных банков Китая.[11] Арест в 2018 г. главного бухгалтера Huawei, имевшего несколько разных паспортов, включая паспорт «общественного лица», который обычно выдают государственным чиновникам, вызывает сомнения в утверждениях о независимости.[12]

Недоверие усиливает и китайская практика кибершпионажа. Критики утверждают, что в Китае не различают военно-политический шпионаж, который ведёт каждая страна, и массовую, экономически мотивированную кражу интеллектуальной собственности у бизнес-конкурентов. Хуже того, КПК делится краденными результатами с китайскими компаниями, что даёт им экономические преимущества, дополняющие щедрые государственные субсидии.[13] Успех Huawei объясняет именно государственная поддержка, поскольку она позволила Huawei быстро развиваться, устранив конкурентов.

---

8 "Who Runs Huawei: Ownership and Governance," *Huawei*, по состоянию на 24 марта 2020, https://www.huawei.com/minisite/who-runs-huawei/en.

9 Christopher Balding and Donald C. Clarke, "Who Owns Huawei?" *SSRN Journal*, April 17, 2019, https://doi.org/10.2139/ssrn.3372669.

10 Bob Seely, Peter Varnish, and John Hemmings, "Defending Our Data: Huawei, 5G and the Five Eyes," *Henry Jackson Society*, Asia Studies Centre, May 16, 2019, p. 26, по состоянию на 1 февраля 2020, https://henryjacksonsociety.org/publications/defendingourdata.

11 RWR Advisory Group, "A Transactional Risk Profile of Huawei," February 13, 2018, p. 20, по состоянию на 17 марта 2020, https://www.rwradvisory.com/wp-content/uploads/2019/03/RWR-Huawei-Risk-Report-2-13-18.pdf.

12 Michael Mui, "How Meng Wanzhou's 'P' Passport Works," *The Star*, January 23, 2019, https://www.thestar.com/vancouver/2019/01/23/how-meng-wanzhous-p-passport-works.html.

13 Su-Mei Ooi and Gwen D'Arcangelis, "Framing China: Discourses of Othering in US News and Political Rhetoric," *Global Media and China* 2, no. 3-4 (2017): 269-283, 275, https://doi.org//10.1177/2059436418756096.

Беспокойство вызывает и возможность Китая принуждать компании к сотрудничеству с разведслужбами. В Законе о разведке 2017 г. есть статьи, которые могут давать китайскими разведслужбами доступ к ИКТ Huawei или право принуждать компанию к сотрудничеству.[14] В частности, основания для контроля приведены в Статье 7. Китай уверяет, что Статья 7 неправильно понята и не угрожает безопасности.[15] В ответ Huawei попросил китайскую юридическую фирму подтвердить это,[16] но критики отмечают, что правовая оценка не устраняет беспокойство.[17] В данный момент есть основания считать, что неисполнение Huawei Статьи 7 испортило бы её отношения с КПК.

Чтобы укрепить доверие к компании, глава Huawei в 2019 г. предложил подписать «соглашение об отказе от шпионажа» с Великобританией, Германией и Индией,[18] но это предложение не вызвало доверия других стран, потому что Huawei не ведёт себя, как частная компания. Например, Huawei утверждает, что избегает публичности по моральным соображениям. Сили, Варниш и Хеммингс[19] подозревают, что реальной причиной может быть «юридическое требование сообщать структуру компании, данные аудита и финансовые отчеты, касающиеся движения денежных средств, капитала и балансов, общественности, акционерам и таким органам, как Комиссия по ценным бумагам и фондовому рынку США». Кроме того, Сили и др.[20] отмечают, что «отсутствие соглашений о сотрудничестве в области безопасности или подобных договоров, в частности, решений о достаточности мер защиты данных» свидетельствует о рисках китайских технологических компаний в данной ситуации.

Всё больше стран запрещают технику Huawei в своих сетях из-за риска, вызванного тесными связями Huawei с КПК и боязнью шпионажа. В настоящее время Huawei запрещён, в частности, в США, Великобритании, Японии, Тайване, Австралии, Новой Зеландии, Швеции, Чехии, Дании, Эстонии, Гернси, Джерси, Латвии, Польше и Румынии. Развивающиеся страны обращают меньше внимания на угрозы безопасности. В большинстве случаев

---

[14] People's Republic of China, National Intelligence Law of the People's Republic, June 27, 2017.

[15] Bonnie Girard, "The Real Danger of China's National Intelligence Law," *The Diplomat*, February 23, 2019, по состоянию на 2 мая 2020, https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law.

[16] Seely, Varnish, and Hemmings, "Defending Our Data: Huawei, 5G."

[17] Samantha Hoffman and Elsa Kania, "Huawei and the Ambiguity of China's Intelligence and Counter-Espionage Laws," *The Strategist* (Australian Strategic Policy Instititute, September 13, 2018, по состоянию на 17 марта 2020, www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws.

[18] "Huawei Answers on Cybersecurity," *Huawei*, October 21, 2019, по состоянию на 26 февраля 2020, https://www.huawei.eu/story/huawei-answers-cybersecurity.

[19] Seely, Varnish, and Hemmings, "Defending Our Data: Huawei, 5G."

[20] Seely, Varnish, and Hemmings, "Defending Our Data: Huawei, 5G."

причина заключается в одновременном предоставлении займов и других форм помощи китайскими государственными организациями,[21] что помогает развивающимся странам преодолеть препятствия для получения технологий.

Пробел: Меры кибердоверия

В отсутствие общепринятых правил страны применяют меры доверия, основанные на нормах контроля обычных вооружений, для укрепления доверия в киберпространстве. Пока что международно признанных обязательных норм приемлемого поведения в этой сфере нет. Международное сообщество согласилось, что существующие международные законы, включая Хартию Организации Объединённых Наций (ООН), действуют и в киберпространстве.[22] Однако нет единства в том, как применять и выполнять эти законы по отношению к конкретным кибероперациям. Одна из причин состоит в том, что существующие законы не рассчитаны на кибердеятельность. Ещё одна причина – отсутствие консенсуса между странами в терминах и определениях, необходимых для выработки приемлемых правил. Часто это объясняется недоверием или отсутствием доброй воли для компромисса со странами-оппонентами из-за нежелания рисковать, доверившись деятелям с иными ценностями.[23]

Меры доверия призваны уменьшить риск или его восприятие, укрепляя доверие и улучшая отношения между странами-участницами. Цель мер кибердоверия – установить стабильные международные отношения и общее понимание приемлемых норм поведения государств в киберпространстве.[24] Они охватывают обмен информацией и сотрудничество стран в борьбе с незаконными кибератаками разных видов.[25] Опираясь на классический контроль вооружений, международные игроки могут оформить меры кибердоверия в виде двусторонних и многосторонних договоров.[26]

---

[21] Cheung, “The Rise of China as a Cybersecurity Industrial Power,” 323.

[22] UN General Assembly, “Developments in the Field of information and Telecommunication in the Context of International Security,” Resolution 70/237 Adopted by the General Assembly on December 23, 2015, по состоянию на 18 марта 2020 (United Nations, 2015), https://undocs.org/en/A/RES/70/237.

[23] Michael Siegrist, George Cvetkovich, and Claudia Roth, “Salient Value Similarity, Social Trust, and Risk/Benefit Perception,” *Risk Analysis: An International Journal* 20, no. 3 (2000): 353-362, https://doi.org//10.1111/0272-4332.203034.

[24] Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013).

[25] Geun Hye Kim, Kyung Bok Lee, and Jong In Lim, “CBMs for Cyberspace beyond the Traditional Environment: Focusing on Features for CBMs for Cyberspace in Northeast Asia,” *The Korean Journal of Defense Analysis* 27, no. 1 (2015): 87-106.

[26] Arnold Kraesten, “Cyber Confidence-Building Measures. Ten Stumbling Blocks Which Complicate the Development and Implementation of Worldwide Politically Acceptable

Они усиливают общее чувство безопасности стран, демонстрируя добрые намерения всех участников.[27] Меры кибердоверия также могут помочь обмену методами и практикой работы, а также взаимным ожиданиям поведения. Поскольку нормы отражают стандарты поведения, ожидаемые от стран в киберпространстве, меры и нормы кибердоверия часто дополняют друг друга.[28]

Меры кибердоверия разработаны для взаимодействия государственных учреждений, поэтому сейчас они не применимы к отношениям государственных и негосударственных субъектов. Большинство экспертов согласны, что меры кибердоверия также должны учитывать многосторонний характер киберпространства, куда входят и частные корпорации.[29] Однако разработкой мер кибердоверия и кибернорм в основном занимаются традиционные межгосударственные международные и региональные организации, такие, как ООН или Организация по безопасности и сотрудничеству в Европе (ОБСЕ).[30] Это имеет смысл для мер доверия, где государства – единственные носители военной и ядерной мощи, но бесполезно в киберпространстве. Здесь власть по умолчанию принадлежит не только государствам, но и технологическим компаниям, которые разрабатывают и эксплуатируют бóльшую часть критической инфраструктуры, включая сети 5G.

Предложение: Расширение мер кибердоверия на негосударственные субъекты

В статье Хитченса и Галлахера сравнивается прогресс работы Группы правительственных экспертов ООН и ОБСЕ по разработке норм и мер кибердоверия в апреле 2019 г. Два момента там представляют ценность для нашей статьи. Во-первых, авторы подчёркивают важность отношений между государственными и негосударственными субъектами, прежде всего – в обмене

Cyber Confidence-building Measures," MSc in Cyber Security, with assistance of Sergej Boeke (The Hague, 2016).

27 Erica D. Borghard and Shawn W. Lonergan, "Confidence Building Measures for the Cyber Domain," *Strategic Studies Quarterly* 12, no. 3 (Fall 2018), по состоянию на 26 декабря 2019, https://www.hsdl.org/?view&did=815333.

28 Patryk Pawlak, "Confidence-Building Measures in Cyberspace: Current Debates and Trends," in *International Cyber Norms: Legal, Policy & Industry Perspectives*, ed. Anna-Maria Osula and Henry Rõigas (Tallinn: NATO CCD COE Publication, (2016), 129-153, https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch7.pdf.

29 Jason Healey, John C. Mallery, Klara J. Tothova, and Nathaniel V. Youd, "Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security," Report (Atlantic Council, November 5, 2014), по состоянию на 30 декабря 2019, https://atlanticcouncil.org/in-depth-research-reports/report/confidence-building-measures-in-cyberspace-a-multistakeholder-approach-for-stability-and-security.

30 Borghard and Lonergan, "Confidence Building Measures for the Cyber Domain."

информацией и оценке риска.[31] Во-вторых, они рекомендуют расширить круг участников за счёт «компаний, владеющих или использующих ключевые компоненты инфраструктуры ИКТ … вместе с некоторыми провайдерами услуг кибербезопасности частного сектора»,[32] в унисон с недавними заявлениями ОБСЕ и Группы правительственных экспертов ООН. В разработке и применении мер кибердоверия должны участвовать и государственные, и негосударственные субъекты, включая частные компании.

В качестве причин нынешнего неучастия ИКТ-сектора в разработке мер кибердоверия приводится «непонимание правительствами киберсферы, ручное регулирование и попытки национальных служб безопасности скомпрометировать инструменты и сети частного сектора в своих интересах».[33] Согласно традиции классических мер кибердоверия, Хитченс и Галлахер призывают развивать сотрудничество для лучшей интеграции частных компаний. Но наша статья предлагает иное толкование описанной в цитате картины. Именно непонимание киберсферы правительствами даёт компаниям возможность скомпрометировать попытки государства регулировать киберпространство. Поэтому страны должны быть заинтересованы в том, чтобы провайдеры ИКТ были не просто участниками процесса мер кибердоверия – они должны стать равноправными субъектами.

В Центре передового опыта совместной защиты от киберугроз НАТО (Cooperative Cyber Defence Centre of Excellence, CCD COE) различают две группы мер кибердоверия. Одна модель основана на спросе, где нормы приемлемого поведения в киберпространстве подстёгивают разработку параллельных мер кибердоверия, что ведёт к росту кибервозможностей. Другая модель основана на предложении – новые кибервозможности, часто разработанные и внедрённые негосударственными субъектами, подстёгивают разработку «конкретных совместных мер доверия для всех сторон».[34] Эти меры кибердоверия ведут к появлению новых норм использования странами новых возможностей.

Павляк планировал использовать негосударственные субъекты для улучшения межгосударственных отношений, но для нашей статьи важно отличие между разными моделями мер кибердоверия. В статье утверждается, что с развитием прорывных технологий в киберпространстве, таких, как 5G, возникает необходимость разработки мер кибердоверия, чтобы снизить риски участников. Как видно из нынешних дебатов о включении или невключении Huawei в сети 5G ряда стран, эти прорывные технологии, не совсем ещё разработанные и даже понятые, уже стали реальностью.

---

[31] Theresa Hitchens and Nancy W. Gallagher, “Building Confidence in the Cybersphere: A Path to Multilateral Progress,” *Journal of Cyber Policy* 4, no. 1 (2019): 4-21, https://doi.org/10.1080/23738871.2019.1599032.

[32] Hitchens and Gallagher, “Building Confidence in the Cybersphere.”

[33] Hitchens and Gallagher, “Building Confidence in the Cybersphere.”

[34] Pawlak, “Confidence-Building Measures in Cyberspace.”

Согласно Пражским предложениям 2019 г., оценка риска должна охватывать потенциальные угрозы технического и нетехнического характера, исходящие от поставщика. Нужно учитывать такие моменты, как правовое поле страны происхождения, форма правления, сотрудничество в области безопасности.[35] Хартия доверия (Charter of Trust, CoT) – консорциум технологических компаний, выступающий за обязательные правила и стандарты – предлагает интересный подход для укрепления доверия между поставщиками ИКТ. Он основан на управлении цепочками поставок и содержит очень важное для этой статьи заявление: «Партнёры по CoT также считают, что никакие незадокументированные функции или возможности удаленного подключения не должны входить в первоначальные настройки устройства, хотя сегодня это еще не является общим правилом».[36] Он признаёт, что не только компании, но и правительства могут оказаться в ситуации, когда присущие ИКТ риски требуют создания правил идентификации и управления доступом.[37]

Появилась тенденция привлекать к регулированию киберпространства зарубежных участников, но включение негосударственных субъектов пока что ограничивается советом и обратной связью. Идея сделать частный сектор партнёром государства при соблюдении мер кибердоверия означает новый подход, о котором совсем недавно упоминалось в отчете Глобальной комиссии по стабильности киберпространства (Global Commission on the Stability of Cyberspace, GCSC), в виде норм киберпространства для государственных и негосударственных субъектов.[38]

Как указано в предыдущем разделе, развитию бизнеса Huawei с рядом стран мешает глубокое недоверие. Позиция Huawei по кибербезопасности показывает, что компания ясно осознаёт это, поскольку целая глава там посвящена «независимости бизнеса». Компания даже заявила о готовности подписать соглашение «об отказе от шпионажа» и скорее закрыться, чем посягнуть на конфиденциальность и безопасность клиентов.[39] Но эта декларация вряд ли убедит критиков, поскольку это – рекламное заявление, не способное серьёзно укрепить доверие, что сделать очень трудно, когда оно

[35] "The Prague Proposals: The Chairman Statement on Cyber Security."

[36] "Charter of Trust Partners Decide on Further Measures for More Cybersecurity," *Charter of Trust*, February 14, 2020, по состоянию на 27 марта 2020, https://www.charteroftrust.com/news/charter-of-trust-partners-decide-on-further-measures-for-more-cybersecurity.

[37] "Our 10 Principles: Cybersecurity Concerns Us All," *Charter of Trust*, по состоянию на 27 марта 2020, https://www.charteroftrust.com/about.

[38] Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, Final Report (Global Commission on the Stability of Cyberspace, November 2019), по состоянию на 1 января 2020, https://cyberstability.org/report/.

[39] "Huawei's Position Paper on Cyber Security."

утрачено.[40] Тут срабатывает упомянутая ранее модель, основанная на предложении. Поскольку новые технологии, предлагаемые Huawei, считаются рискованными, стороны, в частности, заинтересованные страны, должны выработать меры кибердоверия, чтобы устранить риск.

Теперь рассмотрим Центр оценки кибербезопасности (Cyber Security Evaluation Center, HCSEC) Huawei, где тестируют оборудование Huawei и выявляют риски в программном и аппаратном обеспечении, в качестве фундамента для более сложных мер. HCSEC был создан в 2010 г. и укомплектован Huawei, а британский Национальный центр кибербезопасности (National Cyber Security Centre, NCSC) выступал прямым партнёром компании. Наблюдательный совет HCSEC возглавляет глава NCSC, а в его состав входят руководитель Huawei, ряд представителей британского правительства и эксперты частного сектора. Наблюдательный совет с 2014 г. выпускает годовые отчёты, включая аудит, чтобы показать свою независимость от штаб-квартиры Huawei.[41] Цель HCSEC – «показать рост технических возможностей Huawei» и программного обеспечения, но другая его цель – «и далее предоставлять гарантии британскому правительству, обеспечивая открытость, прозрачность и реагирование на вопросы безопасности, возникающие у правительства и британских клиентов»,[42] что соответствует концепции мер кибердоверия. Но анализ технических возможностей сам по себе не устраняет корень проблемы.

В случае Huawei Центр должен решить вопросы реального владения, независимости от влияния КПК и Закона о разведке 2017 г. Эти вопросы связаны со страной происхождения Huawei, что тоже соответствует оценкам риска, изложенным в Пражских предложениях. Хотя HCSEC сообщал об отсутствии свидетельств причастности китайского государства к выявленным техническим недостаткам, это не убедило критиков. Если кто-то считает, что Huawei сотрудничает с КПК и китайскими разведслужбами, отсутствие оборудованного технического «чёрного хода» не будет достаточным доказательством. Учитывая быстрое развитие технологий, кодекс со временем может быть изменен. Непрозрачные отношения между Huawei и китайскими разведслужбами являются серьёзным препятствием для налаживания доверия.

---

[40] Paul Slovic, “Perceived Risk, Trust, and Democracy,” *Risk Analysis: An International Journal* 13, no. 6 (1993): 675-682, https://doi.org/10.1111/j.1539-6924.1993.tb01329.x.

[41] Huawei Cyber Security Evaluation Centre Oversight Board, “Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2020: A Report to the National Security Advisor of the United Kingdom,” Part I: Summary, September 2020, по состоянию на 2 ноября 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923309/Huawei_Cyber_Security_Evaluation_Centre__HCSEC__Oversight_Board-_annual_report_2020.pdf.

[42] Huawei Cyber Security Evaluation Centre Oversight Board, “Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2020,” Part II: Section I.

Политические рекомендации

В статье признаётся, что Huawei, вероятно, не согласится на меры кибердоверия, несмотря на все заявления о стремлении к прозрачности. Но суть статьи не в этом. Она предлагает скорректировать и применить модель, основанную на предложении, как главную меру при выборе страной провайдеров ИКТ. Меры кибердоверия должны укрепить доверие между странами и компаниями ИКТ и способствовать безопасности в киберпространстве, устанавливая нормы прозрачности.

Рекомендация №1: Во-первых, страны должны создать собственные независимые службы корпоративных мер кибердоверия, укомплектованные и руководимые правительственными экспертами в области ИКТ. Задачей этих органов будет проверка потенциальных поставщиков основных ИКТ для страны и оценка связанных с ними рисков. Далее они должны выработать адекватные корпоративные меры кибердоверия для устранения рисков, выявленных в каждой компании. ИКТ-компания, заинтересованная в ведении бизнеса со страной, должна соблюдать меры доверия, чтобы стать поставщиком. Дополнительная выгода корпоративных мер кибердоверия заключается в том, что результатами анализа можно делиться с другими странами, что уменьшит избыточность для ИКТ-компаний. Страны, не способные создать собственную службу, могут брать отчёты о корпоративных мерах кибердоверия других стран за основу для своих контрактов по ИКТ. Или же несколько стран могут объединить ресурсы и создать службы корпоративных мер кибердоверия на региональном уровне. При этом они должны синхронизировать свои будущие стандарты прозрачности и выработать общие условия ведения бизнеса с частными компаниями.

В случае Huawei служба корпоративных мер кибердоверия могла бы выявлять описанные выше риски и разрабатывать меры для их устранения. Один из возможных подходов – условие, чтобы Huawei внедрил меры прозрачности аналогично его европейским конкурентам, Ericsson и Nokia. Как указано в недавнем докладе Strand, эти конкуренты превосходят Huawei по финансовой и технической прозрачности,[43] включая прозрачность использования стороннего кода, что является ещё одной проблемой безопасности базовой программной платформы Huawei, которую чертовски трудно проверить.[44] Ещё одной корпоративной мерой кибердоверия могла бы быть концепция создания национального подразделения Huawei, как целиком отдельного субъекта хозяйствования, которым совместно владеют Huawei и отечественная частная или государственная компания, с серверами внутри страны.

[43] "The Real Cost to Rip and Replace of Chinese Equipment in Telecom Networks."

[44] Jiwon Seo and Monica S. Lam, "InvisiType: Object-Oriented Security Policies" (Stanford University, Computer Systems Laboratory, 2010), p. 1, по состоянию на 7 декабря 2020, https://suif.stanford.edu/papers/ndss10.pdf.

Рекомендация №2: Странам надо предложить это новое расширенное определение мер кибердоверия международным и региональным организациям для признания негосударственных субъектов активными партнерами стран, на которые распространяются меры кибердоверия. Международная организация, например, ООН, может не воспринимать негосударственные субъекты как равных партнёров национальных государств, но такие региональные организации, как ОБСЕ и Организация Американских Государств, должны быть более благосклонны к негосударственным субъектам, поскольку многие механизмы доверия создавались на региональном уровне.

Если такие организации начнут соглашаться с этим расширенным определением мер кибердоверия, это добавит концепции легитимности, мотивируя частные компании приспосабливаться к корпоративным мерам кибердоверия и готовиться, прежде чем предлагать странам вести с ними бизнес. По мере приближения 4-й промышленной революции будет расти зависимость от частного сектора при развитии ИИ, наблюдения, биотехнологий и квантовых исчислений. Эти новые технологии создадут новые вызовы и риски, которые еще предстоит определить и осмыслить. Поскольку многие из этих технологий имеют двойное (военное и гражданское) применение, тем более важно укреплять доверие между странами и частными компаниями, разрабатывающими эти технологии.

Примечание

Представленные здесь взгляды принадлежат исключительно автору и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнерство ради мира», организаций-участниц или издателей Консорциума.

Благодарность

Connections: The Quarterly Journal, Vol. 20, 2021, вышел при поддержке правительства США.

Об авторе

Маттиас Клаус – аналитик в области международной безопасности и рисков. Был командиром отделения, взвода и инструктором Бундесвера, затем поступил на обучение по магистерской программе в области международной безопасности, совместно организованной Центром им. Джорджа Маршалла и Университетом Бундесвера в Мюнхене.
Электронная почта: mk2124@cam.ac.uk