Вестник международных организаций. 2021. Т. 16. № 3. С. 7–33
Научная статья
УДК 327.8:327.7
doi:10.17323/1996-7845-2021-03-01

Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе»[1, 2]

Д.А. Дегтерев, М.С. Рамич, Д.А. Пискунов

Дегтерев Денис Андреевич – д.полит.н., к.э.н., профессор, заведующий кафедрой теории и истории международных отношений Российского университета дружбы народов (РУДН); профессор кафедры мировой экономики МГИМО МИД России; профессор кафедры европейских исследований факультета международных отношений СПбГУ; Российская Федерация, 117198, Москва, ул. Миклухо-Маклая, д. 6; degterev-da@rudn.ru

Рамич Мирзет Сафетович – аспирант кафедры теории и истории международных отношений Российского университета дружбы народов (РУДН); Российская Федерация, 117198, Москва, ул. Миклухо-Маклая, д. 6; ramich_ms@mail.ru

Пискунов Данил Андреевич – студент кафедры теории и истории международных отношений факультета гуманитарных и социальных наук Российского университета дружбы народов (РУДН); Российская Федерация, 117198, Москва, ул. Миклухо-Маклая, д. 6; piskunov_da@mail.ru

Аннотация

С точки зрения теории властного транзита (power transition theory) система международных отношений постепенно входит в фазу «транзита власти», где США, являясь глобальным гегемоном, стремятся сохранить существующий мировой порядок, а КНР создает альтернативные международные форматы для реформирования системы международных отношений и укрепления своей структурной власти. Технологическая сфера и киберпространство становятся полем для несиловой конкуренции между странами, что делает изучение вопросов глобального управления киберпространством критически важным для понимания контуров «новой биполярности».

В статье представлен анализ подходов США и КНР к глобальному управлению киберпространством через призму теории «сетевого общества» Мануэля Кастельса. Авторы поставили задачу определить направления деятельности США и КНР в рамках четырех типов «власти» в киберпространстве: «сетевой власти», «власти сети», «власти в сети» и «сетесозидающей власти».

Проведенный анализ позволяет сделать вывод, что США доминируют в рамках всех четырех типов «власти» за счет функционирования децентрализованной модели, в основе которой лежит принцип «мультистейкхолдеризма», а решающую роль играют негосударственные компании и организации развитых стран. Однако КНР уже подготовила необходимый инструментарий для реформирования существующей системы глобального управления киберпространством на основе централизованной модели с доминирующей ролью ООН в качестве международного органа управления и государства в качестве основного актора. Главными бенефициарами централизованной модели являются развивающиеся страны, которые неспособны оказывать влияние на глобальное управление киберпространством в условиях доминирования частных компаний из развитых стран.

---

[1] Статья поступила в редакцию 10.04.2021.

[2] Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (РФФИ) в рамках научного проекта № 20-514-93003 КАОН_а «Россия и Китай в мировом политическом пространстве: согласование национальных интересов в глобальном управлении».

Ключевые слова: США, КНР, глобальное управление, киберпространство, «сетевое общество», «новая биполярность»

Для цитирования: Дегтерев Д.А., Рамич М.С., Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // Вестник международных организаций. 2021. Т. 16. № 3. С. 7–33 (на русском и английском языках). doi:10.17323/1996-7845-2021-03-01

Введение

В условиях формирования «новой биполярности» между КНР и США вопросы глобального управления получают новый импульс. Фактор ядерного сдерживания постепенно снижает актуальность «силовых» методов борьбы. В этом контексте все большее значение приобретают новые мировые политические пространства, которые становятся ареной геополитического противостояния. Значение киберпространства – одного из таких политических пространств – становится критическим в контексте ускорения процесса цифровизации на фоне пандемии COVID-19. США и КНР, выступая в качестве основных полюсов силы, формируют свои подходы к глобальному управлению киберпространством для контроля над информационными потоками и создания межгосударственных технологических «экосистем». Будучи важной областью глобального управления, управление киберпространством достигает своей цели путем предоставления мировых общественных благ для устранения сбоев в работе правительств и других сетей. Движущей силой киберпространства является главный проводник глобального процесса управления киберпространством или основной поставщик общественных благ в киберпространстве [Yan, 2019].

С точки зрения теории властного транзита (power transition theory) мир вступает в период транзита власти, где КНР, восходящая держава, бросает вызов традиционному гегемону в лице США [Дегтерев, Рамич, Цвык, 2021; Chan, 2019]. Соответственно, в рамках настоящей статьи мы рассматриваем конкуренцию США и Китая за роль *rule-maker* глобального процесса управления в киберпространстве по аналогии с тем, как в рамках теории властного транзита страны конкурируют за место главного проводника общественных благ для системы международных отношений [Organski, 1958; Organski, Kugler, 1980]. В данный момент США являются основой либерального миропорядка и главным проводником общественных благ во всех сферах международного взаимодействия, однако рост неудовлетворенности существующей системой международных отношений среди развивающихся стран и потенциальное нежелание Китая поддерживать существующий мировой порядок в случае успешного транзита власти создают неопределенность в отношении будущего системы международных отношений [Nye, 2020].

В рамках глобального управления киберпространством существуют два наиболее актуальных подхода: «мультистейкхолдеризм», или децентрализованная модель управления Интернетом с ведущей ролью НКО, которую поддерживают США и развитые страны [Kleinwächter, 2007; Carr, 2015; Hofmann, 2016; Strickling, Hill, 2017; Mueller, 2020; Васильковский, Игнатов, 2020], и централизованная модель управления киберпространством с ключевой ролью государства, которую поддерживают Китай и развивающиеся страны [Galloway, Baogang, 2014; Arsène, 2016; Zeng, Stevens, Chen, 2017; Hong, Harwit, 2020; Bi, 2020; Cai, 2021]. В существующей литературе подробно рассмотрены

принципы и основы двух подходов, однако недостаточное внимание уделяется практическим и теоретическим аспектам конкуренции двух стран за лидерство в глобальном управлении киберпространством.

США играют ключевую роль в управлении киберпространством по ряду причин. Во-первых, именно в США созданы первые протоколы функционирования сети Интернет. Во-вторых, в США уже создана система управления Интернетом. В 1998 г. в Калифорнии была зарегистрирована некоммерческая организация Internet Corporation for Assigned Names and Numbers (ICAAN) (Корпорация по управлению доменными именами и IP-адресами) [Демидов, 2017]. В ходе создания организации между ICAAN и Министерством торговли был подписан Меморандум о взаимопонимании, который закреплял реализацию ряда функций в рамках компетенции Корпорации, однако до 2016 г. ICAAN оставалась подотчетной правительству США [Васильковский, Игнатов, 2020, с. 16]. В 2016 г. функция управления доменами верхнего уровня и IP-адресами перешла полностью под юрисдикцию ICAAN [ICAAN, 2016]. Таким образом, основные задачи модели США – концентрирование функций управления критической инфраструктурой в руках частных компаний и создание инклюзивного процесса управления киберпространством, который реализуется некоммерческой организацией ICAAN.

Решающий вклад, определивший основу глобального управления киберпространством, был сделан на Всемирных встречах по вопросам Интернета в 2003 и 2005 гг. На Всемирном саммите было выработано определение термина «глобальное управление Интернетом», смысл которого сводился к участию различных акторов, в том числе государств, общественных организаций, научного и технического сообщества. Ключевой результат – учреждение Форума по управлению Интернетом (IGF), ставшего координационным и консультативным органом [Van Eeten, Mueller, 2013, p. 724]. В результате Всемирного саммита оформились принципы модели, учитывающей интересы всех заинтересованных сторон, – мультистейкхолдеризма (multistakeholderism) [Carr, 2015]. С продлением мандата Форума по управлению Интернетом в 2015 г. политика формирования глобального управления киберпространством с участием всех заинтересованных сторон сохранилась на десять лет [Якушев, 2016].

Альтернативный подход к управлению киберпространством, реализуемый КНР, опирается на государственный суверенитет в вопросе управления внутренним сегментом сети Интернет, ограничивая технологическое влияние и роль негосударственных акторов в управлении киберпространством. В рамках данного подхода основой глобального управления является ООН, а в процесс принятия решений должны быть вовлечены все государства на равной основе, в то время как международные некоммерческие организации играют консультативную роль при принятии решений [Зиновьева, 2015, с. 116; Wang, 2020]. Особое место в рамках рассматриваемой модели занимает принцип суверенитета в информационном или киберпространстве, который предполагает контроль государства над внутренней сетью Интернет [Shen, 2016, p. 319]. Основой китайского подхода является формирование сообщества единой судьбы в сетевом пространстве на базе «четырех принципов» и «пяти предложений», выдвинутых Си Цзиньпином в 2015 г. на 2-й Всемирной конференции по управлению Интернетом [Li, 2020, p. 27].

Вопрос управления киберпространством мы рассматриваем в контексте теории власти в сетевом обществе, в которой главной функцией государства становится контроль над телекоммуникационной индустрией и информацией. Методологической основой исследования является теория «сетевого общества» Мануэля Кастельса (см. разд. «Глобальное управление киберпространством в рамках теории “сетевого общества”»). Данная статья призвана стать аналитической рамкой для сравнения подходов США (разд. «Подход США к управлению глобальным киберпространством – многосторон-

няя децентрализованная модель») и КНР (разд. «Подход КНР к управлению киберпространством – многосторонняя централизованная модель») к глобальному управлению киберпространством и сопоставить их с практическими шагами в рамках стратегической конкуренции двух стран (разд. «Практическое измерение конкуренции США и КНР в киберпространстве»). В заключительном разделе статьи изложены основные отличительные черты подходов двух стран и даны комментарии относительно контуров «новой биполярности» в рамках глобального управления киберпространством (разд. «Контуры системы глобального управления киберпространством: конкуренция подходов»).

Глобальное управление киберпространством в рамках теории «сетевого общества»

Методологической основой исследования является теория «сетевого общества», предложенная М. Кастельсом в работе «Власть коммуникации» [Castells, 2009]. Формирование и осуществление власти и властных отношений в государстве изменилось с появлением технологий коммуникации. Опора государственной власти, кроме насилия и внушения страха, – это контроль над мыслями и восприятием. Такой контроль осуществляется через конструирование в сознании общества образа государства, значения власти и властных отношений. Ключевая идея теории заключается в том, что власть базируется на контроле над коммуникацией и информацией, которая охватывает «сетевое общество» [Castells, 2007].

Развитие ИКТ способствовало созданию «сетевого общества» как на мировом уровне, так и на государственном. В рамках такого «сетевого общества» все узлы, создающие сеть общества, связаны массовой коммуникацией. Коммуникация, в свою очередь, строится на мультимедийных сетях, которые содержат стандарты или протоколы коммуникации.

Кастельс выделяет четыре вида власти, которые объясняют осуществление власти в глобальном обществе. Первый вид власти – сетевая власть – характеризуется тем, что управление находится в руках акторов или организаций, формирующих ядро сети. Власть основывается на функции включения/исключения [Castells, 2011]. Например, с помощью создания и распространения социальной сети телекоммуникационные компании могут укрепить свою властную позицию, а затем, используя стратегии гейткипинга, закрыть доступ тем, кто не разделяет ценности или подвергает опасности интересы, которые доминируют в программах этой сети.

Второй вид власти – власть сети – характеризуется установлением правил включения в сети или выработки протоколов коммуникации. По мнению М. Кастельса, власть сети исходит из двух вещей: популярности тех или иных протоколов и правил коммуникации и отсутствия альтернативы. Власть определяется установлением глобальных правил коммуникации и включения в сеть, которых придерживается большинство акторов [Castells, 2011]. Примером такой власти является технологическое лидерство западных стран в создании сервисов электронной коммерции и других ИТ-услуг, предложения технологических стандартов коммуникации и в целом определение правил управления киберпространством по западному образцу. Фактически крупные ИТ-компании преследуют цель интеграции всех сервисов в единую сетевую «экосистему», которая будет ограничивать выбор пользователя.

Третий вид власти – власть в сети. По М. Кастельсу, власть в сети, тем более в доминантной сети, является реляционной, так как ключевой актор, обладающий наи-

большей властью, пользуется возможностью навязывать свою волю. Такая власть конструируется через институты доминирования [Castells, 2011]. Следует отметить, что данный вид власти США используют для продвижения своих правил и принципов устройства и эволюции сети Интернет, так как такие международные организации, как ICAAN, IGF, WSIS, IETF, соблюдают ключевые принципы модели США.

Четвертый вид – сетесозидающая власть. Данный вид власти основывается на действии двух механизмов: программирования целей и принципов сети и управления массовой коммуникацией. Программирование сети устанавливает цель, идею, фреймы и концепции, которые являются продуктами культуры и используются в процессе коммуникации. Программирование сети – это создание идентичности, идеологии [Castells, 2011]. Данный вид власти был применен в ходе избирательной кампании Барака Обамы, основой которой стала коммуникация посредством использования сети Интернет.

Согласно данной теории, контроль над коммуникацией в сетевом обществе является неотъемлемым атрибутом власти государства, с помощью которого конструируется образ самого государства. Сетевая власть развивается на нескольких уровнях, начиная от индивидуального и заканчивая национальным и глобальным. Доминирование нескольких подходов в рамках глобальной системы становится причиной технологического разделения стран мира, подобного разделению пользователей, выбирающих сетевые «экосистемы» в рамках национального рынка технологических решений.

Подход США к управлению глобальным киберпространством – многосторонняя децентрализованная модель

США как создатель сети Интернет и ее инфраструктуры играют ведущую роль в глобальном управлении Интернетом. Впервые позиция США по управлению киберпространством была отмечена в заявлении Министерства торговли США от 1998 г. В заявлении отмечалось, что реализация функций управления частными компаниями предпочтительнее для развития сети Интернет как децентрализованной системы, поощряющей свободу личности и отсутствие государственного контроля [NTIA, 1998]. Тем самым управление киберпространством изначально рассматривалось как децентрализованная система, основанная на деятельности частных компаний и некоммерческих организаций.

Согласно Международной стратегии США для киберпространства 2011 г., администрация Б. Обамы придерживалась принципов свободы в сети Интернет, продвижения многосторонней модели управления Интернетом в рамках негосударственных структур. Потоки информации в сети Интернет, согласно позиции США, не должны быть ограничены или не должны подвергаться регулированию. Вопрос управления критическими ресурсами подразумевает многосторонний процесс принятия решения с участием частных организаций, что обеспечит стабильность и безопасность критической инфраструктуры сети Интернет [The White House, 2011].

Управление киберпространством основывается на децентрализованной архитектуре, состоящей из негосударственных организаций и компаний, таких как Форум по управлению Интернетом (IGF), Корпорация по управлению доменными именами и IP-адресами (ICAAN) и Инженерный совет Интернета (IETF) [Strickling, Hill, 2017, p. 299]. ICAAN и IETF отвечают за технические аспекты управления. Так, Инженерный

совет отвечает за разработку и обновление основных технических стандартов Интернета. Участниками организации могут быть все заинтересованные лица. В рамках IGF государства выступают наравне с другими акторами. Тем самым стирается граница между теми, кто устанавливает правила в киберпространстве (rule-maker), и теми, кто эти правила принимает (rule-taker) [Hofmann, Katzenbach, Gollatz, 2017, p. 1410]. В контексте теории «сетевого общества» данные организации составляют третий вид власти – власть в сети. Деятельность IGF, IETF, ICAAN основана в первую очередь на принципе участия всех заинтересованных сторон, что способствует признанию подхода США.

Отдельным аспектом власти США в «сетевом обществе» является администрирование критических ресурсов сети Интернет. Управление ключевой интернет-инфраструктурой, в том числе корневыми серверами DNS, осуществляется государственными организациями США и частными компаниями, некоммерческими организациями, университетами и интернет-провайдерами. Так, операторами десяти корневых серверов являются Вооруженные силы США, Министерство обороны США и Национальное агентство по аэронавтике и исследованию космического пространства (NASA), университет Южной Калифорнии, Мэрилендский университет, а также такие НКО, компании и интернет-провайдеры, как VeriSign, Cogent Communications, ICAAN, Internet Systems Consortium [IANA, 2021]. Таким образом, обладая доступом к управлению критическими ресурсами сети Интернет, США получают власть в создании и определении правил включения и других стандартов сети Интернет.

В обновленной Стратегии кибербезопасности от 2018 г., принятой при администрации Дональда Трампа, в разделе «Принцип IV. Продвижение американского влияния» США осуждают попытки установления контроля над внутренней сетью Интернет, нарушая принцип открытого и свободного Интернета [Department of Defense, 2018]. Тем самым это делает возможным проникновение иностранных телекоммуникационных компаний во внутреннюю сеть и распространение иностранного влияния на общество той или иной страны. В указанной стратегии США придерживаются многосторонней модели управления Интернетом, в рамках которой необходимо противостоять созданию государственно ориентированной инфраструктуры, создающей контроль над сетью Интернет [Department of Defense, 2018].

С другой стороны, модель управления киберпространством, в которой главную роль играют государства, отвергается. Так, в ходе слушаний в Палате представителей Конгресса США в 2012 г. была выдвинута резолюция, в которой глобальное управление сетью Интернет под руководством МСЭ усилит контроль государств по этому вопросу, а многосторонняя модель, продвигаемая США, потеряет силу [US Congress, 2012]. Вследствие передачи контроля МСЭ одно государство будет иметь один голос, чтобы выразить свою волю по вопросам управления киберпространством [DeNardis, 2014, p. 33].

Важную роль в сетевой власти США и поддержании международного статуса лидера в киберпространстве играют телекоммуникационные корпорации Google, Apple, Facebook, Amazon, Microsoft (GAFAM), занимающие главенствующее положение в мире в качестве поисковых сервисов, социальных сетей, сервисов электронной коммерции и производства операционных систем [Moore, 2016, p. 15]. Данные компании образуют экосистему приложений, которая используется как на общественном, так и на государственном уровне. Так, поисковая система Google занимает более 60% рынка поисковых систем в мире [GlobalStats, 2021]. Компания Facebook охватывает 70% рынка социальных сетей, уступая социальным сетям только в ряде стран [GlobalStats, 2021a]. В свою очередь, корпорации Apple, Google, Microsoft охватывают более 70% рынка операционных систем в мире [GlobalStats, 2021b].

Именно телекоммуникационные корпорации занимаются разработкой технических протоколов коммуникации и функционирования социальных приложений сети Интернет. Тем самым технологические корпорации формируют глобальную сеть влияния как на безопасность государств, так и на мировое общество в целом [Slaughter, 2009, p. 98]. Показательным примером власти частных организаций является кейс с программой разведки PRISM, которую проводило правительство США совместно с крупнейшими частными технологическими корпорациями, такими как Google, Apple, Skype, Facebook и др. [Hill, 2014, p. 87]. С точки зрения теории «сетевого общества» монопольное положение телекоммуникационных компаний формирует первый тип власти США в глобальной сети – сетевую власть.

Открытое киберпространство, на котором настаивают США, наилучшим образом способствует распространению влияния США в контексте технологической зависимости и информационного влияния на мировое информационное пространство с помощью СМИ, технологических компаний, регулирующих потоки информации в социальных сетях и других приложениях, и частных компаний, управляющих критической инфраструктурой сети Интернет.

Рассматривая позиционные документы модели США, необходимо обратиться к Будапештской конвенции о киберпреступности. Конвенция не только приводит к гармонизации законодательств подписавших ее стран, но и дает право на трансграничный сбор и использование данных без уведомления об этом того или иного государства. Конвенция подписана преимущественно странами с высоким уровнем ВНД, в то время как развивающиеся страны, или страны глобального Юга, воздержались от ее ратификации. Обеспечивая безграничный доступ к данным, промышленно развитые государства получают данные, обрабатываемые с помощью алгоритмов ИИ, которые выявляют слабые места национальных технологических компаний. Тем самым технологические компании-лидеры, получая потоки обрабатываемой информации, влияют на конкурентоспособность национальных компаний в частности и на развитие государства в целом.

В качестве международных документов, соответствующих модели глобального управления США, необходимо отметить Декларацию принципов построения информационного общества 2003 г. [ООН, 2003], Тунисскую программу информационного общества 2005 г. [ООН, 2005]. Оба документа заложили основу нынешней системы глобального управления – рыночные силы являются движущей силой развития сети Интернет, Интернет признается открытым пространством, а глобальное управление осуществляется с участием всех заинтересованных акторов.

На Глобальном многостороннем саммите по вопросу о будущем управления Интернетом, прошедшем в 2014 г. в Бразилии, был принят документ, включивший основные принципы многостороннего управления и дорожную карту управления Интернетом [NETmundial, 2014]. В отличие от документов, принятых на Всемирной встрече на высшем уровне по вопросам информационного общества, в финальном документе саммита в Бразилии были рассмотрены проблемы национального и регионального управления Интернетом.

Таким образом, США реализуют подход через многосторонние организации, отвечающие за принятие протоколов и развитие архитектуры Интернета, и форматы, в которых негосударственные акторы принимают участие наравне с представителями правительств. Центральные функции управления Интернетом и критическими ресурсами находятся под контролем зарегистрированных в США некоммерческих организаций. Посредством работы такого механизма США сохраняют сложившуюся систему управления киберпространством и свое влияние в ней.

Подход КНР к управлению киберпространством – многосторонняя централизованная модель

Изучение подхода КНР к управлению киберпространством необходимо начать с принципов регулирования внутренней, или национальной, сети. Так как развитие сети Интернет и сферы ИКТ привело к увеличению роли и влияния негосударственных акторов на мировую политику и национальную безопасность государств, вопросы информационной и кибербезопасности для КНР вышли на первый план. В «Белой книге» Китая 2010 г. администрирование сети Интернет рассматривается как важная функция в обеспечении национальной безопасности, а инфраструктурные объекты, сайты и в целом сеть Интернет, расположенная на территории КНР, находятся под юрисдикцией Китая [People's Republic of China, 2010]. Подход КНР к управлению киберпространством основывается на поддержании легитимности и экономического роста [Jiang, 2010, p. 72].

Важным аспектом в осуществлении внутренней политики в информационном пространстве является технологическая основа. В 2016 г. КНР приняла «Национальную стратегию информатизации и развития», в которой описаны этапы становления КНР «сильным сетевым государством». Один из этапов, реализуемых до 2025 г., – повышение конкурентоспособности китайских технологических компаний в мире и создание передовой сети мобильной связи, функционирующей на китайском ПО и сетевых приложениях [Понька, Рамич, У, 2020, с. 385].

Функционирование внутренней сети осуществляется на основе экосистемы приложений китайских телекоммуникационных компаний. Национальные компании КНР (Alibaba, Tencent, Baidu, Huawei, China Mobile) являются опорой для власти государства в обществе, так как они обеспечивают работу поисковой системы (Baidu), функционирование социальной сети (Tencent), ведение электронной коммерции в государстве (Alibaba), производство сетевого, телекоммуникационного оборудования (Huawei) и обеспечение мобильной связи (China mobile). Эти компании составляют ядро национальной сети КНР и обладают функциями ее регулирования. Правительство КНР тем самым получает доступ к управлению национальным сегментом сети Интернет и с точки зрения теории регулирует сети коммуникации. Таким образом, государство получает контроль над техническими функциями управления сетью Интернет и осуществляет социальное управление в обществе на основе регулирования содержания информационных потоков.

Одним из аспектов суверенитета в киберпространстве является независимость государства от продуктов и услуг иностранных компаний и развитие национальных телекоммуникационных компаний и инфраструктуры, в том числе разработка и использование собственного ПО, создание системы волоконно-оптических кабелей, локализация данных [Кутюр, Тоупин, 2020, с. 56]. Более того, управление сетью Интернет согласуется с традицией социального управления и государственного администрирования. Социальное управление с развитием ИКТ трансформировалось из полицейского надзора и жесткой репрессивной политики в системное идеологическое формирование общества, необходимого для поддержки режима партии. Такая политика приводит к управлению Интернетом, с одной стороны, посредством блокировки, цензуры и фильтрации и, с другой стороны, путем распространения идеологической информации [Yang, 2014, p. 111]. Таким образом, КНР использует государственно ориентированную модель управления внутренней сетью Интернет для поддержания стабильности и создания идей и образов, транслируемых в общество посредством коммуникационных сетей.

Принципы администрирования внутренней сети Интернет транслируются на международный уровень в государственных стратегиях КНР по глобальному управлению киберпространством. Основой глобального управления КНР является теория гармоничного мира, предложенная Ху Цзиньтао, и концепция «сообщества единой судьбы человечества», предложенная Си Цзиньпином. Теория гармоничного мира предусматривает создание общества государств на основе взаимного сотрудничества с целью обеспечить общее развитие и безопасность. Согласно данной теории, приоритет в решении международных споров отдается ООН [Grachikov, 2020, p. 140]. В то же время внимание к формированию «сообщества единой судьбы человечества» в киберпространстве усилилось в период пандемии, когда большую часть времени люди во всем мире стали проводить в сети [Cai, 2021].

Основой политики КНР является Стратегия международного сотрудничества в киберпространстве [Ministry of Foreign Affairs of People's Republic of China, 2017]. В документе отмечены ключевые принципы политики КНР в киберпространстве. Согласно указанным в Стратегии принципам, необходимо обеспечить мир и безопасность, предотвратить гонку вооружений и конфликт в киберпространстве. Важную роль в Стратегии играет принцип суверенитета, который включает право на выбор модели управления сетью и модели государственной политики в сети Интернет. В дополнение к этому выделяется совместное управление киберпространством как принцип, в котором ООН является ключевым инструментом управления. В заключительной части выделяется принцип всеобщего доступа, направленный на ликвидацию цифрового разрыва между развитыми и развивающимися государствами. В контексте теории «сетевого общества» сетевая власть правительства КНР, реализуемая посредством деятельности национальных телекоммуникационных компаний, является основным средством поддержания общественной стабильности и экономического роста.

Подход КНР к глобальному управлению киберпространством характеризуется установленными в Стратегии задачами, среди которых выделены признание суверенитета государства в информационном пространстве и невмешательство во внутренние дела государства, создание кодекса правил и принципов поведения государств в киберпространстве. В отношении США китайские эксперты придерживаются мнения, что развитые страны во главе с США проводят политику сетевого гегемонизма, создавая условия, в которых развивающиеся страны не принимают участия в глобальном управлении Интернетом [Li Chuanjun, Li Huaiyang, 2018, p. 15]. В этих условиях развитые страны и их технологические корпорации получают возможность контролировать киберпространство под эгидой модели мультистейкхолдеризма.

КНР определяет глобальное управление киберпространством как многостороннюю, прозрачную систему управления Интернетом, функционирующую на основе Организации Объединенных Наций. В такой системе государства играют определяющую роль, а негосударственным акторам и заинтересованным сторонам отводится консультативная роль. Важным аспектом управления Интернетом является распределение и совместное управление критической информационной инфраструктурой, такой как корневые серверы Интернета [Li Chuanjun, Li Huaiyang, 2018, p. 18].

Модель глобального управления Интернетом, которой придерживается Китай, предусматривает распространение и применение правил, регулирующих международные отношения, к управлению киберпространством. Ключевая роль в такой модели отводится государствам, обладающим суверенитетом над внутренним сегментом сети Интернет. Процесс принятия решений осуществляется рамках Международного союза электросвязи (далее – МСЭ) и ООН, в которых развивающиеся и развитые государства могут принять равное участие в решении вопросов.

Присутствие КНР в МСЭ примечательно с точки зрения широкого участия представительства правительства, бизнеса и академического сообщества [Negro, 2020, p. 109]. Правительство КНР представлено Министерством промышленности и информатизации. Позицию частных организаций представляют более 40 телекоммуникационных компаний КНР. Академическое сообщество представлено техническими вузами и университетами КНР [ITU, 2021].

Для достижения своих целей КНР развивает сотрудничество в рамках двусторонних и многосторонних форматов, способствует вовлечению менее развитых государств в процесс формирования глобального управления киберпространством и создает коалиции государств.

В рамках Шанхайской организации сотрудничества государства-члены в 2011 г. ратифицировали Соглашение о сотрудничестве в области обеспечения международной информационной безопасности [МИД России, 2009], определив такие принципы, как невмешательство в информационные ресурсы других государств и интернационализацию управления глобальной сетью Интернет. Соглашение стало большим шагом вперед в формировании общей позиции государств, так как в рамках документа было осуществлено создание нормативно-правовой базы понятий, раскрывающих ключевые термины в киберпространстве, определение угроз и рисков, а также закрепление информационного пространства государства как сферы, находящейся под юрисдикцией государства.

Более того, позиция КНР по вопросу создания общего правового регулирования схожа с позицией Российской Федерации. Между правительствами государств подписано Соглашение о сотрудничестве в сфере международной информационной безопасности [Правительство России, 2015]. В качестве документов, направленных на регулирование информационного пространства, Российская Федерация предложила две конвенции, соблюдающие принципы суверенитета в информационном пространстве, и модель государственного управления национальным сегментом сети Интернет: Конвенция (концепция) об обеспечении международной информационной безопасности [МИД России, 2011] и Конвенция по институционализации вопросов регулирования безопасного функционирования и развития сети Интернет на основе равноправного участия мирового сообщества в управлении глобальной сетью [Минкомсвязь России, 2017] (Конвенция безопасного функционирования и развития сети Интернет). Оба документа были предложены в качестве концепций в ООН. Основные принципы конвенций были соблюдены в инициативе государств – членов ШОС в «Правилах поведения в области обеспечения международной информационной безопасности» [Суворов, 2020]. Принятие единых правил поведения в рамках ООН позволит превратить киберпространство из «серой зоны» международных отношений в комфортное правовое поле, что позволит избежать последствий геополитической конфронтации между крупнейшими технологическими акторами [Chen, 2020, p. 95–97]. КНР и Российская Федерация в рамках глобального управления киберпространством отдают приоритет таким коллективным механизмам регулирования, как ООН и МСЭ. ООН является центральной площадкой для выработки МИБ, МСЭ – альтернативным институтом управления киберпространством с увеличением суверенного контроля над национальным сегментом Интернета [Ларионова, Шелепов, 2021].

Созданная Пекином в 2014 г. Всемирная конференция по вопросам Интернета в Учжене стала площадкой для обмена мнениями между государствами и участниками, желающими пересмотреть нынешний порядок глобального управления. В 2015 г. лидер КНР Си Цзиньпин отметил, что сеть Интернет должна регулироваться в соответствии с теми же принципами, что и другие сферы международных отношений, тем

самым настаивая на ключевых принципах политики КНР по данному вопросу. Повесткой саммитов 2019 и 2020 гг. стала инициатива «построения сообщества единой судьбы в киберпространстве» [WIC, 2020]. В рамках инициативы поставлены задачи как экономического и технологического сотрудничества, в том числе распространение технологий 5G, так и осуществления совместного управления Интернетом с руководящей ролью ООН [WIC, 2020]. Данная инициатива направлена на объединение развивающихся стран для противостояния модели управления глобальным киберпространством, основанной на принципах США [Hong, Harwit, 2020, p. 3].

Тем самым Китай реализует задачи, поставленные в рамках указанного подхода, через международные правительственные организации, консультационные и совещательные форматы. В рамках таких форматов согласуется общая позиция по вопросам глобального управления киберпространством и развития Интернета. В результате работы указанного многостороннего механизма были приняты совместный проект конвенции ООН, декларации ШОС и БРИКС о МИБ, а также двусторонние соглашения в области формирования правил поведения в киберпространстве.

Таким образом, модель глобального управления киберпространством, продвигаемая КНР, основывается на принципах суверенитета, равного участия всех государств в процессе принятия решений, ведущей роли ООН в процессе управления критическими ресурсами и киберпространством. Данная модель управления соответствует политике, проводимой КНР на государственном уровне.

В условиях ускорения темпов цифровизации Китаю необходимо одновременно решать несколько задач: формировать образ ответственного государства на международной арене и продвигать свои технологические компании на глобальном рынке, совершенствовать систему управления киберпространством на национальном уровне и создавать благоприятные условия для развития на международном уровне [Zhu, Liu, 2021].

Практическое измерение конкуренции США и КНР в киберпространстве

Киберпространство стало одним из ключевых «полей» стратегической конкуренции США и КНР. В борьбе за лидерство в киберпространстве важную роль играют телекоммуникационные корпорации, так как они являются и драйверами экономического развития, и ключевыми акторами для лидерства обоих государств в киберпространстве [Данилин, 2020, с. 109]. Соответственно, США и КНР прибегают к политике ограничения влияния телекоммуникационных компаний ввиду угрозы национальной безопасности. В контексте теории «сетевого общества» государство стремится закрепить контроль над потоками информации и протоколами коммуникации между «узлами сети».

ICAAN играет ключевую роль в глобальном управлении киберпространством. В деятельность НКО активно вовлечены представители США и КНР. Среди 75 компаний, аккредитованных в качестве регистраторов доменов верхнего уровня (gTLD)[3], 46 компаний США [ICAAN, n. d., a]. В правительственный консультативный комитет входят три представителя из Национального управления по телекоммуникации и информации и два эксперта из Министерства торговли США. В консультативный комитет системы корневых серверов, который также принимает участие в формировании

[3] gTLD – это одна из категорий доменов верхнего уровня (TLD), поддерживаемых Администрацией адресного пространства Интернета (IANA) для использования в системе доменных имен в Интернете.

политики НКО, входят представители компаний – операторов корневых серверов [ICAAN, n. d., c]. С другой стороны, в ICAAN аккредитованы восемь китайских компаний [ICAAN, n. d., a]. В Правительственном консультативном комитете присутствуют четыре представителя Министерства промышленности и информационных технологий КНР и два исследователя Академии информационных и коммуникационных технологий КНР [ICAAN, 2021 n. d., c].

В рамках системы обеспечения информационной безопасности КНР применяет фильтрацию потоков информации и запрещает деятельность иностранных компаний. Ключевой элемент такой системы – файрволл (firewall), его цель состоит в опеспечении безопасности от внешних угроз [Понька, Рамич, У, 2020]. Под запрет попали такие компании, как Facebook (включая Instargram, WhatsApp, Messenger), Google (включая все сервисы Google), Twitter, Snapchat, Dropbox и др. Иные корпорации вынуждены соблюдать жесткую систему правил функционирования приложений. Так, Apple пришлось исключить ряд приложений из магазина приложений AppStore ввиду их влияния на национальную безопасность КНР, в том числе HKMap Live, Quartz, Clubhouse. Первые два приложения использовались протестующими в 2019 г. в Гонконге. В дополнение к ограничению иностранного влияния в рамках своего информационного пространства, КНР ограничила использование программного обеспечения Windows в государственных компьютерных системах, альтернативой стала Ubuntu Kylin, основанная на Linux OS. В качестве альтернативы ПО для мобильных устройств КНР разрабатывает Harmony OS. Тем самым КНР ограничивает влияние социальных сетей, новостных агентств и иностранных ИТ-компаний на свое общество, запрещает использование приложений, программного обеспечения и оборудования, которые собирают и обрабатывают данные пользователей и могут оказывать влияние на социальные настроения в обществе.

С другой стороны, в ходе торговой войны США ввиду угрозы национальной безопасности запретили функционирование приложений, социальных сетей, сервисов электронной коммерции и использование оборудования китайских компаний, которые имели связи с НОАК. Политика санкций и блокировки в отношении китайских компаний началась в 2018 г. на первом этапе торговой войны, когда Министерство торговли США приняло запрет на экспорт комплектующих компонентов и программного обеспечения, необходимого для телекоммуникационного оборудования ZTE [BIS, 2018]. В дополнение к этому Министерство обороны США опубликовало список компаний, которые прямо или косвенно взаимодействуют с НОАК КНР [Department of Defense, 2021]. В список вошли следующие компании: Huawei, China Telecom, China Mobile, Xiaomi. Это стало причиной для применения санкций в отношении Huawei на экспорт комплектующих и использование сервисов экосистемы Google в устройствах, производимых под брендом компании. Huawei получила запрет на размещение своего оборудования на территории США, главным образом это касалось инфраструктуры 5G и системы видеонаблюдения. На том же основании Федеральная комиссия по связи США отклонила заявку китайской компании China Mobile на предоставление услуги мобильной телекоммуникации на территории США [FCC, 2019]. В январе 2021 г. в черный список китайских компаний, сотрудничающих с НОАК, была включена компания Xiaomi. Это, в свою очередь, повлекло за собой запрет на экспорт технологий американских компаний и инвестиций. В марте 2021 г. Xiaomi смогла успешно обжаловать включение компании в черный список и тем самым добилась снятия ограничений на инвестиции [Xiaomi, 2021]. Обжалование приговора стало первым подобным прецедентом в ходе торговой войны США и КНР.

В дополнение к перечисленным выше ограничениям на деятельность китайских технологических гигантов США запретили функционирование китайских сервисов электронной коммерции, приложений и социальных сетей. На первом этапе указом президента США Д. Трампа были запрещены социальные сети Wechat (Tencent) и Tiktok (ByteDance) [Executive Office of the President, 2020]. Капитализация компаний сократилась на 100 млн долл. [Дмитриев, 2020, с. 72]. Схожие меры были применены в отношении небанковских платежных систем Alipay, CamScanner, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat Pay и WPS Office [Executive Office of the President, 2021]. В обоих случаях санкции против приложений были обоснованы тем, что телекоммуникационные компании могут собирать и обрабатывать обширные массивы информации пользователей (big data), а также подвергать цензуре политический контент, создаваемый пользователями. Китайские эксперты охарактеризовали продолжающуюся конфронтацию в технологическом пространстве как «цифровую холодную войну», результат которой определит, какой из подходов будет доминировать в глобальном управлении Интернетом в ближайшие десятилетия [Xu, 2021].

По-прежнему актуальной в рамках конкуренции США и КНР остается гонка технологических компаний за распространение 5G-технологий. Лидерами в развертывании оборудования 5G являются Huawei, ZTE, Ericsson и Nokia. Так, технологии компании Huawei используются и тестируются в 68 странах, в то время как другая китайская компания ZTE предоставляет свое оборудование 5G 28 странам. С другой стороны, европейские компании Ericsson и Nokia сотрудничают с 42 и 46 странами соответственно. Несмотря на то что американские компании напрямую не являются полноценными участниками глобальной гонки по развертыванию сетей 5G, США поддерживают европейских партнеров путем санкционного давления на китайские компании, выступая «единым фронтом» развитых стран.

Конкуренция между компаниями обострилась в августе 2020 г. после заявления Майка Помпео о реализации программы Clean Network, ключевая цель которой состоит в ограничении деятельности китайских компаний в рамках пяти направлений: предоставление ИКТ-услуг, установка и использование китайских программных приложений, хранение и обработка облачных данных, создание системы волоконно-оптических кабелей [Department of State, 2020]. Государства, присоединяющиеся к данной программе, сокращают присутствие китайских телекоммуникационных компаний на своем рынке и отказываются от технологий 5G. Так, по данным Госдепартамента США, к программе присоединилось около 53 государств, в том числе государства – члены НАТО и ЕС и участники альянса «Пять глаз» [Department of State, 2020]. Именно с момента принятия данной программы началась «цифровая холодная война» между США и КНР [Xu, 2021, p. 19].

Принятие данной программы сказалось на деятельности китайских компаний в мире. Так, в 2019 г. Huawei развивала 5G-сети в Греции и планировала запустить коммерческое использование сетей в 2020 г. [Michalopoulos, 2019]. Но в сентябре 2020 г. после визита М. Помпео Греция присоединилась к программе и сделала выбор в пользу Ericsson [Department of State, 2020]. Подобная ситуация наблюдается во многих государствах, присоединившихся к программе США. В дополнение к этому Европейский союз выработал Инструментарий для безопасности 5G, в рамках которого определены стандарты и критерии безопасности для сетей 5G [European Commission, 2020]. Тем самым компании Ericsson и Nokia получат преимущество на европейском рынке 5G. В рамках программы выделены компании, использование услуг и оборудования которых не угрожает безопасности государства, там же обозначены критерии и меры без-

опасности для предотвращения проникновения на рынок поставщиков «с высоким уровнем риска».

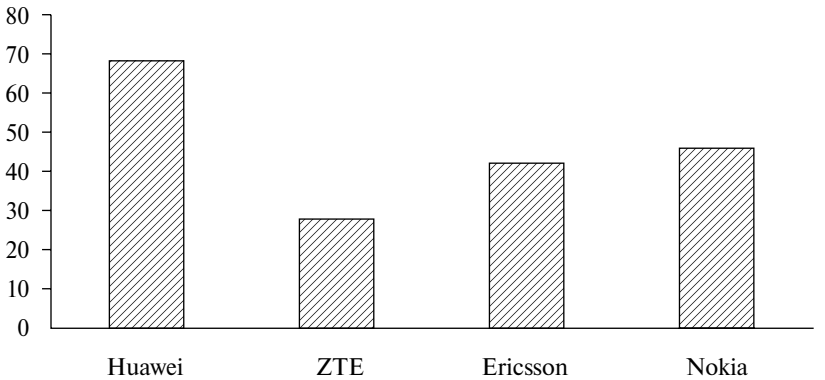

Рис. 1. Число подписанных соглашений в сфере 5G по странам

Источники: Составлено авторами на основе данных [Ericsson, 2021; Nokia, 2021; Huawei, 2021; ZTE, 2021].

Таким образом, проблема управления киберпространством в контексте власти в сетевом обществе выходит на первый план в новом биполярном противостоянии США и КНР. Принятие той или иной модели обеспечит абсолютное лидерство и влияние какой-либо державы в мире. США, будучи гегемоном как в рамках традиционной системы международных отношений, так и в рамках киберпространства, поддерживают и развивают существующую модель власти «в Интернете» и «через Интернет», и их поддерживают развитые страны. Китай объединяет вокруг себя развивающиеся страны, заинтересованные в легитимизации и уравнивании в правах всех стран в рамках глобального управления [Zhao, 2021, p. 50–51]. Несмотря на это, следует признать, что китайские эксперты предлагают реформировать международную систему управления киберпространством «по китайскому образцу» [Zhao, 2021, p. 59].

Контуры системы глобального управления киберпространством: конкуренция подходов

Различия подходов США и КНР к глобальному управлению киберпространством, показанные в табл. 1, позволяют сделать вывод о том, что Китай уже сформировал полный набор альтернативных инструментов для реализации своего подхода к глобальному управлению в киберпространстве, в то время как США стремятся использовать форматы, созданные ранее для сохранения лидирующей позиции в данном политическом пространстве.

Существующая модель управления киберпространством функционирует на основе принципов, которые были разработаны еще в конце XX в. Управление и развитие сети Интернет и сферы ИКТ обеспечивается за счет рыночных механизмов, то есть взаимодействия между негосударственными акторами, такими как ICAAN, VeriSign, Cogent Communications и т.д. Более того, установленные при создании ICAAN принципы свободной и открытой сети Интернет позволяют технологическим корпорациям и СМИ США распространять свое влияние, тем самым создавая уникальные префе-

ренциальные условия для США в сфере глобального управления киберпространством. Основными бенефициарами децентрализованной модели являются развитые страны, на территориях которых расположены крупнейшие ИТ-корпорации мира, позволяющие им использовать «власть в сети» для продвижения своих интересов.

С другой стороны, Китай предлагает альтернативный подход, в котором доля рыночных сил значительно меньше. Процессы администрирования внутренней сети выполняются государством в соответствии с его внутренним законодательством. Вопросы глобального управления Интернетом главным образом должны решаться в ООН, в том числе в рамках МСЭ. Это позволит избежать влияния технологических компаний на решение вопросов, связанных с глобальным управлением, и обеспечить равное участие всех государств. На данном этапе КНР создает альтернативные площадки для продвижения своей позиции среди развивающихся стран, в том числе проводит Всемирную конференцию в Учжене.

В пользу неизбежности трансформаций глобальной системы управления киберпространством говорит и соотношение пользователей Интернета: жители развитых стран составляют около трети от общего числа пользователей Интернета, тогда как на долю развивающихся стран приходится две трети от общего числа пользователей [Li, 2020]. При этом около половины населения развивающихся стран не имеет доступа в Интернет, и это означает, что одновременно с цифровизацией доля этих стран будет увеличиваться. Вместе с тем будет увеличиваться и поддержка китайских идей трансформации международной системы управления киберпространством.

Пандемия COVID-19 ускорила процесс цифровизации и выявила уязвимости существующей системы глобального управления киберпространством. Государства оказались не готовы к тому, что люди будут проводить больше времени в сети, чем вне ее. Это породило такой феномен, как «цифровой авторитаризм», и в очередной раз доказало опасность «цифрового разрыва» между развитыми и развивающимися странами [Cai, Wang, 2021, p. 5–8]. Кризис открыл для США и КНР новые возможности для реализации своих глобальных проектов в цифровом пространстве, которые привели к новому витку конкуренции в рамках формирования «новой биполярности».

Таблица 1. Подходы США и КНР к глобальному управлению киберпространством

	США	**КНР**
Модель управления Интернетом	Многосторонняя модель управления киберпространством с широким участием негосударственных, частных и общественных организаций (multistakeholder)	Многосторонняя модель управления киберпространством с ведущей ролью государств в рамках ООН (multilateral)
Модель управления информационным пространством	Открытое интернет-пространство, основанное на децентрализованной структуре	Государственно ориентированная модель с упором на суверенитет
Ключевые органы в управлении киберпространством	ICAAN, IETF	ООН/МСЭ
Международные площадки по управлению Интернетом	Форум по управлению Интернетом (IGF)	Всемирная конференция по вопросам Интернета в Учжене

	США	КНР
Позиционные документы	**Национальный уровень**: Национальная стратегия кибербезопасности США 2011 г.; Национальная стратегия по кибербезопасности США 2018 г. **Международный уровень**: Будапештская конвенция по борьбе с киберпреступностью; Декларация принципов построения информационного общества; Тунисская программа для информационного общества; Итоговый документ Глобального многостороннего саммита в Бразилии 2014 г.	**Национальный уровень**: Белая книга КНР; Международная стратегия сотрудничества в киберпространстве; Стратегия информатизации и развития **Международный уровень**: Соглашение о сотрудничестве в области обеспечения международной информационной безопасности ШОС; Конвенция о международной информационной безопасности 2011 г.; Конвенция безопасного функционирования и развития сети Интернет 2017 г.
Роль телекоммуникационных компаний	Телекоммуникационные компании как ключевой актор развития и управления киберпространством	Телекоммуникационные компании как акторы, осуществляющие политику государства в киберпространстве

Источник: Составлено авторами.

***

В статье исследована проблема противостояния подходов США и КНР к глобальному управлению через призму теории «сетевого общества» М. Кастельса. Согласно теории, власть государства претерпевает изменения в технологическом контексте и получает новые инструменты осуществления. В итоге можно сделать следующие выводы.

В пространстве «сетевой власти», где разворачивается конкуренция за создание глобального «сетевого общества», в котором акторы реализуют стратегию гейткипинга (включения и выключения из глобальной сети), лидируют США, так как корпорации группы GAFAM занимают монопольное положение на рынках технологий. КНР создает альтернативную сеть, функционирующую на своей экосистеме приложений, которая не имеет глобального распространения, однако снижает зависимость национальной сети от международного контекста.

Аналогичным образом США занимают лидирующее положение в рамках «власти сети», где конкуренция между двумя державами осуществляется за определение протоколов коммуникации, принципов управления критическими ресурсами Интернета и реализацию функции распределения доменных адресов, так как в настоящее время большая часть этих функций разделена между организациями, расположенными в США и развитых странах. КНР стремится реформировать существующий порядок и добивается осуществления функций управления критической инфраструктурой под руководством ООН при определяющей роли государства.

Контроль над «властью в сети» осуществляется через создание институтов глобального управления киберпространством. Существующие институты глобального управления Интернетом (ICAAN, IGF, WSIS, IETF) функционируют в соответствии с принципами модели глобального управления США. С другой стороны, КНР про-

двигает свои институты и органы глобального управления Интернетом, одновременно создавая альтернативу выбора и основу для параллельного существования двух систем.

США и КНР стремятся получить возможность определять принципы коммуникации в глобальной сети, устанавливать цели и направления глобального взаимодействия для лидерства в рамках «сетесозидающей власти». Каждая из держав создает свою сеть, основанную на принципах глобального управления киберпространством, которые дают им широкие возможности для развития в будущем. Участниками таких сетей становятся все страны мира, вынужденные делать выбор в условиях формирования «новой биполярности».

Список источников

Васильковский С.А., Игнатов А.А. (2020). Управление Интернетом: системные диспропорции и пути их разрешения // Вестник международных организаций. Т. 15. № 4. С. 7–29. doi:10.17323/1996-7845-2020-04-01.

Данилин И.В. (2020). Влияние цифровых технологий на лидерство в глобальных процессах: от платформ к рынкам? // Вестник МГИМО-Университета. Т. 13. № 1. С. 100–116. doi:10.24833/2071-8160-2020-1-70-100-116.

Дегтерев Д.А., Рамич М.С., Цвык В.А (2021). США – КНР: транзит власти и контуры «конфликтной биполярности» // Вестник Российского университета дружбы народов. Сер. Международные отношения. Т. 21. № 2. С. 210–231. doi:10.22363/2313-0660-2021-21-2-210-231.

Демидов О. (2017). Глобальное управление Интернетом и безопасность в сфере использования ИКТ: ключевые вызовы для мирового сообщества. М.: Альпина Паблишер.

Дмитриев С.С. (2020). Американо-китайское технологическое соперничество: от «высокомерия» к бойкоту // Мировая экономика и международные отношения. Т. 64. № 12. С. 70–77.

Зиновьева Е.С. (2015). Глобальное управление Интернетом: российский подход и международная практика // Вестник МГИМО-Университета. Т. 43. № 4. С. 111–118.

Кутюр С., Тоупин С. (2020). Что означает понятие «суверенитет» в цифровом мире? // Вестник международных организаций. Т. 15. № 4. С. 48–69. doi:10.17323/1996-7845-2020-04-03.

Ларионова М.В., Шелепов А.В. (2021). Формирующиеся механизмы регулирования цифровой экономики. Риски и возможности для многосторонней системы глобального управления // Вестник международных организаций. Т. 16. № 1. doi:10.17323/1996-7845-2021-01-02.

МИД России (2009). Многосторонние договоры. Режим доступа: https://www.mid.ru/ru/foreign_policy/international_contracts/multilateral_contract/-/storage-viewer/multilateral/page-1/50243 (дата обращения: 06.04.2021).

МИД России (2011). Конвенция об обеспечении международной информационной безопасности. Режим доступа: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения: 06.04.2021).

Минкомсвязь России (2017). Концепция безопасного функционирования и развития сети «Интернет». Режим доступа: https://digital.gov.ru/uploaded/files/prilozheniekontseptsiikonventsiioon.docx (дата обращения: 06.04.2021).

ООН (2003). Декларация принципов. Построение информационного общества – глобальная задача в новом тысячелетии / Всемирная встреча на высшем уровне по вопросам информационного общества. Женева, 2003 – Тунис, 2005. Режим доступа: https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (дата обращения: 06.04.2021).

ООН (2005). Тунисская программа для информационного общества / Всемирная встреча на высшем уровне по вопросам информационного общества. Женева, 2003 – Тунис, 2005. Режим доступа: https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (дата обращения: 06.04.2021).

Понька Т.И., Рамич М.С., У Ю. (2020). Информационная политика и информационная безопасность КНР: развитие, подходы и реализация // Вестник Российского университета дружбы народов. Сер. Международные отношения. Т. 20. № 2. С. 382–394. doi:10.22363/2313-0660-2020-20-2-382-394

Правительство России (2015). Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области информационной безопасности. Режим доступа: http://static.government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf (дата обращения: 06.04.2021).

Суворов А. (2020). Современные реалии киберпространства: Россия как ведущий игрок в обеспечении международной информационной безопасности. Режим доступа: http://www.pircenter.org/blog/view/id/433 (дата обращения: 06.04.2021).

Якушев М.В. (2016). Итоги Всемирной встречи на высшем уровне по вопросам информационного общества // Пульс Кибермира. Т. 10. № 1.

Arsène S. (2016). Global Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic World Order? // China Perspectives. Vol. 106. No. 2. P. 25–35. https://doi.org/10.4000/chinaperspectives.6973

Bi S. (2020). Yingdui "Niquanqiuhua" Zhongguo Quanqiu Wangluokongjian Zhili Linian De Chuanbo [Responding to "Counter-Globalization": The Spread of China's Global Cyberspace Governance Philosophy]. China Publishing. P. 50–53. (In Chinese)

Bureau of Industry and Security (BIS) (2018). ZTE Order Terminating Denial Order. Режим доступа: https://www.bis.doc.gov/index.php/documents/pdfs/2246-zte-order-terminating-denial-order (дата обращения: 06.04.2021).

Cai C. (2021). Promoting the building of a community of destiny in cyberspace // China Social Science Journal. Vol. 1. No. 8. P. 10–12. (In Chinese.

Cai C., Wang T. (2021). Global Cyber Governance in the Context of COVID-19: Opportunities and Challenges // International Forum. Vol. 23. No. 1. P. 3–17. (In Chinese)

Carr M. (2015). Power plays in global internet governance // Millennium. Vol. 43. No. 2. P. 640–659. https://doi.org/10.1177%2F0305829814562655.

Castells M. (2007). Communication, power and counter-power in the network society // International journal of communication. Vol. 1. No. 1. P. 238–266. Режим доступа: https://ijoc.org/index.php/ijoc/article/view/46/35 (дата обращения: 18.08.2021).

Castells M. (2009). Communication Power. Oxford University Press.

Castells M. (2011). Network theory: A network theory of power // International journal of communication. Vol. 5. P. 773–787. Режим доступа: https://ijoc.org/index.php/ijoc/article/view/1136/553 (дата обращения: 18.08.2021).

Chan S. (2019). More Than One Trap: Problematic Interpretations and Overlooked Lessons from Thucydides. Journal of Chinese Political Science. Vol. 24. No 1. P. 11–24. http://dx.doi.org/10.1007/s11366-018-9583-2.

Chen W. (2020). Cyberspace and its security in a geopolitical context // Academia. Vol. 261. No. 2. P. 87–97. (In Chinese)

Denardis L. (2014). The global war for internet governance. Yale University Press. P. 288.

Ericsson (2021). Режим доступа: https://www.ericsson.com/en (дата обращения: 06.04.2021).

European Commission (2020). Secure 5G networks: Questions and Answers on the EU toolbox. Режим доступа: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127 (дата обращения: 06.04.2021).

Executive Office of the President (2020). Addressing the Threat Posed by TikTok, and Taking Additional Steps to Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain. Executive Order 13942, 6 August. Режим доступа: https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency (дата обращения: 06.04.2021).

Executive Office of the President (2021). Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies. Executive Order 13971, 5 January. Режим доступа: https://

www.federalregister.gov/documents/2021/01/08/2021-00305/addressing-the-threat-posed-by-applications-and-other-software-developed-or-controlled-by-chinese (дата обращения: 06.04.2021).

Federal Communications Commission (FCC) (2019). FCC Denies China Mobile Telecom Services Application. News Release, 9 May. Режим доступа: https://www.fcc.gov/document/fcc-denies-china-mobile-telecom-services-application (дата обращения: 06.04.2021).

Galloway T., Baogang H. (2014). China and Technical Global Internet Governance: Beijing's Approach to Multi-Stakeholder Governance within ICANN, WSIS and the IGF // China: An International Journal. Vol. 12. No. 3. P. 72–93.

GlobalStats (2021). Browser Market Share Worldwide. Режим доступа: https://gs.statcounter.com/ (дата обращения: 06.04.2021).

GlobalStats (2021a). Social Media Stats Worldwide. Режим доступа: https://gs.statcounter.com/social-media-stats (дата обращения: 06.04.2021).

GlobalStats (2021b). Operating System Market Share Worldwide. Режим доступа: https://gs.statcounter.com/os-market-share#monthly-202002-202102-bar (дата обращения: 06.04.2021).

Grachikov E.N. (2020). China in Global Governance: Ideology, Theory, and Instrumentation // Russia in Global Affairs. No. 4. P. 132–153. http://dx.doi.org/10.31278/1810-6374-2020-18-4-132-153.

Hill R. (2014). Internet Governance: The Last Gasp of Colonialism, or Imperialism by Other Means? The Evolution of Global Internet Governance / R. Radu, J.M. Chenou, R. Weber (eds). Berlin: Springer. https://doi.org/10.1007/978-3-642-45299-4_5.

Hofmann J. (2016). Multi-stakeholderism in Internet governance: putting a fiction into practice // Journal of Cyber Policy. Vol. 1. No. 1. P. 29–49. https://doi.org/10.1080/23738871.2016.1158303.

Hofmann J., Katzenbach C., Gollatz K. (2017). Between coordination and regulation: Finding the governance in Internet governance // New Media & Society. Vol. 19. No. 9. P. 1406–1423. http://dx.doi.org/10.1177/1461444816639975.

Hong Y., Harwit E. (2020). China's globalizing internet: history, power, and governance // Chinese Journal of Communication. Vol. 13. No. 1. P. 1–7. https://doi.org/10.1080/17544750.2020.1722903.

Huawei (2021). Режим доступа: https://www.huawei.com (дата обращения: 06.04.2021).

International Telecommunication Union (ITU) (n. d.). China. Режим доступа: https://www.itu.int/online/mm/scripts/gensel9?_ctryid=1000100502 (дата обращения: 06.04.2021).

Internet Assigned Numbers Authority (IANA) (n. d.). List of Root Servers. Режим доступа: https://www.iana.org/domains/root/servers (дата обращения: 06.04.2021).

Internet Corporation for Assigned Names and Numbers (ICAAN) (2016). NTIA IANA Functions' Stewardship Transition. Режим доступа: https://www.icann.org/stewardship (дата обращения: 06.04.2021).

Internet Corporation for Assigned Names and Numbers (ICAAN) (n. d., a). List of Accredited Registrars. Режим доступа: https://www.icann.org/en/accredited-registrars?filter-letter=a&sort-direction=desc&sort-param=name&page=1 (дата обращения: 06.04.2021).

Internet Corporation for Assigned Names and Numbers (ICAAN) (n. d., b). GAC Membership. Режим доступа: https://gac.icann.org/about/members# (дата обращения: 06.04.2021).

Internet Corporation for Assigned Names and Numbers (ICAAN) (n. d., c). Root Server System Advisory Committee. Режим доступа: https://www.icann.org/groups/rssac (дата обращения: 06.04.2021).

Jiang M. (2010). Authoritarian informationalism: China's approach to internet sovereignty // SAIS Review of International Affairs. Vol. 30. No. 2. P. 71–89. http://dx.doi.org/10.1353/sais.2010.0006.

Kleinwächter W. (2007). The Power of Ideas: Internet Governance in a Global Multi Stakeholder Environment // Marketing für Deutschland.

Li C., Li H. (2018). Global governance of the Internet based on sovereignty in cyberspace // E-Government. Vol. 185. No. 5. P. 9–17. (In Chinese)

Li H. (2020). "Digital Silk Road" and the Reconstruction of Global Cyberspace Governance // International Forum. Vol. 21. No. 6. P. 42–44. (In Chinese)

Li Z., Tang R. (2020). Multi-stakeholder Model: Path to Build Global Internet Governance System // Media Observer. Vol. 444. No. 12. P. 21–28. (In Chinese)

Michalopoulos S. (2019). Huawei Official: 5G Is a "Historic" Opportunity for Greece and Cyprus // Euroactiv. 30 July. Режим доступа: https://www.euractiv.com/section/5g/news/huawei-official-5g-is-a-historic-opportunity-for-greece-and-cyprus/ (дата обращения: 06.04.2021).

Ministry of Foreign Affairs of People's Republic of China (PRC) (2017). International Strategy of Cooperation on Cyberspace. Режим доступа: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml (дата обращения: 06.04.2021).

Moore M. (2016). Tech giants and civic power // Centre for the study of Media, Communication & Power, King's College London. Retrieved February. Vol. 5. P. 88. Режим доступа: https://www.kcl.ac.uk/policy-institute/assets/cmcp/tech-giants-and-civic-power.pdf (дата обращения: 19.08.2021).

Mueller M.L. (2020). Against Sovereignty in cyberspace // International Studies Review. Vol. 22. No. 4. P. 779–801. https://doi.org/10.1093/isr/viz044.

National Telecommunications and Information Administration (NTIA) (1998). Statement of Policy on the Management of Internet Names and Addresses. Режим доступа: https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses (дата обращения: 06.04.2021).

Negro G. (2020). A history of Chinese global Internet governance and its relations with ITU and ICANN // Chinese Journal of Communication. Vol. 13. No. 1. P. 104–121. https://doi.org/10.1080/17544750.2019.1650789.

NETMundial (2014). The Global Multistakeholder Meeting on the Future of Internet Governance. Режим доступа: https://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (дата обращения: 06.04.2021).

Nokia (2021). Режим доступа: https://www.nokia.com (дата обращения: 06.04.2021).

Nye J.S. (2020). "Power and Interdependence with China" // The Washington Quarterly. Vol. 43. No. 1. P. 7–21. https://doi.org/10.1080/0163660X.2020.1734303.

Organski A.F.K. (1958). World Politics. N.Y.: A. Knopf.

Organski A.F.K., Kugler J. (1980). The war ledger. Chicago: The University of Chicago Press.

People's Republic of China (2010). White paper on the Internet in China. Режим доступа: https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm (дата обращения: 06.04.2021).

Shen H. (2016). China and global internet governance: toward an alternative analytical framework // Chinese Journal of Communication. Vol. 9. No. 3. P. 304–324. https://doi.org/10.1080/17544750.2016.1206028.

Slaughter A.M. (2009). America's edge: Power in the networked century // Foreign affairs. P. 94–113. Режим доступа: https://www.jstor.org/stable/20699436 (дата обращения: 06.04.2021).

Strickling L.E., Hill J.F. (2017). Multi-stakeholder internet governance: successes and opportunities // Journal of Cyber Policy. Vol. 2. No. 3. P. 296–317. https://doi.org/10.1080/23738871.2017.1404619.

The White House (2011). International Strategy for Cyberspace. Режим обращения: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата обращения: 06.04.2021).

United States Congress (2012). House of Representatives. Committee on Energy and Commerce. International Proposals to Regulate the Internet Режим доступа: https://archive.org/details/gov.gpo.fdsys.CHRG-112hhrg79558/page/n11/mode/2up (дата обращения: 06.04.2021).

United States Department of Defense (2018). Summary: Department of Defense Cyber Strategy. Режим доступа: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (дата обращения: 06.04.2021).

United States Department of Defense (2021). List of Additional Companies, in Accordance With Section 1237 of FY99 NDAA. News Release. 14 January. Режим доступа: https://www.defense.gov/Newsroom/Releases/Release/Article/2472464/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/ (дата обращения: 06.04.2021).

United States Department of State (n. d.). The Clean Network. Режим доступа: https://2017-2021.state.gov/the-clean-network/index.html (дата обращения: 06.04.2021).

van Eeten M.J.G., Mueller M. (2013). Where is the governance in Internet governance? // New media & society. Vol. 15. No. 5. P. 720–736. https://doi.org/10.1177%2F1461444812462850.

Wang Z. (2020). The new dynamics of global cyberspace rule-making under the UN dual-track system // China Information Security. Vol. 20. No. 1. P. 40–43. (In Chinese)

World Internet Conference (WIC) (2020). Initiative on Jointly Building a Community With a Shared Future in Cyberspace. Режим доступа: http://www.wuzhenwic.org/2020-11/18/c_564467.htm (дата обращения: 06.04.2021).

Xiaomi (2021). Statement. Режим доступа: https://blog.mi.com/en/2021/03/14/statement/ (дата обращения: 06.04.2021).

Xu P. (2021). Global Internet Governance towards Digital Cold War or Digital Commons // Information Security and Communications Privacy. Vol. 21. No. 3. P. 16–23. (In Chinese)

Yan L. (2019). Global Cyberspace Governance: State Actors and the China – US Cyber Relationship // Contemporary International Relations. Vol. 29. No. 2. P. 105–124. Режим доступа: http://www.cicir.ac.cn/UpFiles/file/20200227/637184169973143065186752 2.pdf (дата обращения 19.08.2021).

Yang G. (2014). The return of ideology and the future of Chinese Internet policy // Critical Studies in Media Communication. Vol. 31. No. 2. P. 109–113. https://doi.org/10.1080/15295036.2014.913803.

Zeng J., Stevens T., Chen Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty" // Politics & Policy. Vol. 45. No. 3. P. 432–464. https://doi.org/10.1111/polp.12202.

Zhao R. (2021). Global Network Governance Reform: Path Choices for Rising Powers // Academia. Vol. 272. No. 1. P. 50–59. (In Chinese).

Zhu D., Liu Y-W. (2021). The Legal Governance System of Cyberspace in the Community of Shared Future of Mankind and China's Plans // Journal of Yangtze Normal University. Vol. 37. No. 1. P. 30–39. (In Chinese)

ZTE (2021). Режим доступа: https://www.zte.com.cn/ (дата обращения: 06.04.2021).

International Organisations Research Journal, 2021, vol. 16, no 3, pp. 7–33
Original article
doi:10.17323/1996-7845-2021-03-01

U.S. & China Approaches to Global Internet Governance: "New Bipolarity" in Terms of "The Network Society"[1, 2]

D. Degterev, M. Ramich, D. Piskunov

Denis Degterev – Dr. of Sc. (Political Science), PhD in Economics, Professor, Head, Department of Theory and History of International Relations, RUDN University; Professor, World Economy Department, MGIMO University; Professor, Department of European Studies, St. Petersburg State University; 6 Miklukho-Maklaya Ulitsa, Moscow, 117198, Russian Federation; degterev-da@rudn.ru

Mirzet Ramich – PhD candidate, Department of Theory and History of International Relations, RUDN University; 6 Miklukho-Maklaya Ulitsa, Moscow, 117198, Russian Federation; ramich_ms@mail.ru

Danil Piskunov – Student of the Department of Theory and History of International Relations, RUDN University; 6 Miklukho-Maklaya Ulitsa, Moscow, 117198, Russian Federation; piskunov_da@mail.ru

Abstract

From the perspective of power transition theory, international relations system is gradually entering the phase of "power transition" where the United States, as a global hegemon, seeks to maintain the existing world order, and China establishes alternative international formats to reorganize the system of international relations and strengthen its structural power. Cyberspace and technological sphere are becoming the field of non-violent competition between states, which makes the study of global governance of cyberspace critical for the understanding of the outlines of the "new bipolarity".

The analysis in the paper is focused on U.S. & China approaches to global governance of cyberspace through the prism of Manuel Castells' theory of "network society". The authors aimed to determine the directions of the U.S. and China policy in the course of four types of "power" in cyberspace: networking power, network power, networked power and network-making power.

Present analysis concludes that the United States play crucial role in the course of all four types of "power" at the expense of decentralized model of Internet governance which is based on the idea of "multistakeholderism". NGO and other entities play a decisive role in such a model. Nonetheless, China has already developed necessary tools for reforming the present system of global governance of cyberspace based on centralized model with the leading role of United Nations as an international governance organization and state as a basic actor. The main beneficiaries of the centralized model are developing countries, which are unable to influence the global governance of cyberspace under the dominance of private companies from developed countries.

Keywords: U.S., China, global governance, cyberspace, "network society", "new bipolarity"

For citation: Degterev D., Ramich M., Piskunov D. U.S. & China Approaches to Global Internet Governance: "New Bipolarity" in Terms of "The Network Society". *International Organisations Research Journal*, 2021, vol. 16, no 3, pp. 7–33 (in English). doi:10.17323/1996-7845-2021-03-01

References

Arsène S. (2016). Global Internet Governance in Chinese Academic Literature: Rebalancing a Hegemonic World Order? *China Perspectives*, vol. 106, no 2, pp. 25–35. https://doi.org/10.4000/chinaperspectives.6973.

[1] This article was submitted 10.04.2021.

[2] The reported study was funded by RFBR within research project № 20-514-93003 "Russia and China in the global political space: harmonization of national interests in global governance".

Bi S. (2020). Yingdui "Niquanqiuhua" Zhongguo Quanqiu Wangluokongjian Zhili Linian De Chuanbo [Responding to "Counter-Globalization": The Spread of China's Global Cyberspace Governance Philosophy]. China Publishing, pp. 50–3. (In Chinese)

Bureau of Industry and Security (BIS) (2018). ZTE Order Terminating Denial Order. Available at: https://www.bis.doc.gov/index.php/documents/pdfs/2246-zte-order-terminating-denial-order (accessed 6 April 2021).

Cai C. (2021). Promoting the Building of a Community of Destiny in Cyberspace. *China Social Science Journal*, vol. 1, no 8, pp. 10–2. (In Chinese)

Cai C., Wang T. (2021). Global Cyber Governance in the Context of COVID-19: Opportunities and Challenges. *International Forum*, vol. 23, no 1, pp. 3–17. (In Chinese)

Carr M. (2015). Power Plays in Global Internet Governance. *Millennium*, vol. 43, iss. 2, pp. 640–59. https://doi.org/10.1177%2F0305829814562655.

Castells M. (2007). Communication, Power and Counter-Power in the Network Society. *International Journal of Communication*, vol. 1, pp. 238–66. Available at: https://ijoc.org/index.php/ijoc/article/view/46/35 (accessed 18 August 2021).

Castells M. (2009). *Communication Power*. Oxford University Press.

Castells M. (2011). Network Theory: A Network Theory of Power. *International Journal of Communication*, vol. 5, pp. 773–87. Available at: https://ijoc.org/index.php/ijoc/article/view/1136/553 (accessed 18 August 2021).

Chan S. (2019). More Than One Trap: Problematic Interpretations and Overlooked Lessons From Thucydides. *Journal of Chinese Political Science*, vol. 24, no 1, pp. 11–24. Available at: http://dx.doi.org/10.1007/s11366-018-9583-2.

Chen W. (2020). Cyberspace and Its Security in a Geopolitical Context. *Academia*, vol. 261, no 2, pp. 87–97. (In Chinese)

Couture S., Toupin S. (2020). Chto oznachaet ponjatie "suverenitet" v cifrovom mire? [What Does the Notion of "Sovereignty" Mean When Referring to the Digital?]. *International Organisations Research Journal,* vol. 15, no 4, pp. 48–69. https://doi.org/10.17323/1996-7845-2020-04-03.

Danilin I.V. (2020). Vlijanie cifrovyh tehnologij na liderstvo v global'nyh processah: ot platform k rynkam? [The Impact of Digital Technologies on Leadership in Global Processes: From Platforms to Markets?] *MGIMO Review of International Relations*, vol. 13, no 1, pp. 100–16. https://doi.org/10.24833/2071-8160-2020-1-70-100-116

Degterev D.A., Ramich M.S., Cvyk V.A (2021). U.S. – China: "Power Transition" and the Outlines of "Conflict Bipolarity." *Vestnik RUDN: International Relations,* vol. 21, no 2, pp. 210–31. https://doi.org/10.22363/2313-0660-2021-21-2-210-231

Demidov O. (2017). *Global'noye upravleniye Internetom i bezopasnost' v sfere ispol'zovaniya IKT: Klyuchevyye vyzovy dlya mirovogo soobshchestva* [*Global Internet Governance and ICT Security: Key Challenges for the Global Community*]. Moscow: Al'pina Publisher. (In Russian)

Denardis L. (2014). *The Global War for Internet Governance*. Yale University Press. Available at: https://www.jstor.org/stable/j.ctt5vkz4n.

Dmitriev S. (2020). Amerikano-kitajskoe tehnologicheskoe sopernichestvo: ot "vysokomerija" k bojkotu [U.S. – China Technological Rivalry: From "Arrogance" to Boycott]. *World Economy and International Relations*, vol. 64, no 12, pp. 70–7. https://doi.org/10.20542/0131-2227-2020-64-12-70-77.

Ericsson (2021). Available at: https://www.ericsson.com/en (accessed 6 April 2021).

European Commission (EC) (2020). Secure 5 Networks: Questions and Answers on the EU Toolbox. 29 July. Available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127 (accessed 6 April 2021).

Executive Office of the President (2020). Addressing the Threat Posed by TikTok, and Taking Additional Steps to Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain. Executive Order 13942, 6 August. Available at: https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency (accessed 6 April 2021).

Executive Office of the President (2021). Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies. Executive Order 13971, 5 January. Available at: https://www.federalregister.gov/documents/2021/01/08/2021-00305/addressing-the-threat-posed-by-applications-and-other-software-developed-or-controlled-by-chinese (accessed 6 April 2021).

Federal Communications Commission (FCC) (2019). FCC Denies China Mobile Telecom Services Application. News Release, 9 May. Available at: https://www.fcc.gov/document/fcc-denies-china-mobile-telecom-services-application (accessed 6 April 2021).

Galloway T., Baogang H. (2014). China and Technical Global Internet Governance: Beijing's Approach to Multi-Stakeholder Governance Within ICANN, WSIS and the IGF. *China: An International Journal*, vol. 12, no 3, pp. 72–93. Available at: https://muse.jhu.edu/article/563560 (accessed 19 August 2021).

GlobalStats (2021a). Browser Market Share Worldwide. Available at: https://gs.statcounter.com/ (accessed 6 April 2021).

GlobalStats (2021b). Social Media Stats Worldwide. Available at: https://gs.statcounter.com/social-media-stats (accessed 6 April 2021).

GlobalStats (2021c). Operating System Market Share Worldwide. Available at: https://gs.statcounter.com/os-market-share#monthly-202002-202102-bar (accessed 6 April 2021).

Grachikov E.N. (2020). China in Global Governance: Ideology, Theory, and Instrumentation. *Russia in Global Affairs*, no 4, pp. 132–53. http://dx.doi.org/10.31278/1810-6374-2020-18-4-132-153.

Government of the Russian Federation (2015). Soglasheniye mezhdu Pravitel'stvom Rossiyskoy Federatsii i Pravitel'stvom Kitayskoy Narodnoy Respubliki o sotrudnichestve v oblasti informatsionnoy bezopasnosti [Agreement Between the Russian Government and the Government of the People's Republic of China on Co-operation in the Field of International Information Security]. Available at: http://static.government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf (accessed 6 April 2021). (In Russian)

Hill R. (2014). Internet Governance: The Last Gasp of Colonialism, or Imperialism by Other Means? *The Evolution of Global Internet Governance* (R. Radu, J.M. Chenou, R. Weber (eds)). Berlin: Springer. https://doi.org/10.1007/978-3-642-45299-4_5.

Hofmann J. (2016). Multi-Stakeholderism in Internet Governance: Putting a Fiction Into Practice. *Journal of Cyber Policy*, vol. 1, iss. 1, pp. 29–49. https://doi.org/10.1080/23738871.2016.1158303.

Hofmann J., Katzenbach C., Gollatz K. (2017). Between Coordination and Regulation: Finding the Governance in Internet Governance. *New Media & Society*, vol. 19, iss. 9, pp. 1406–23. http://dx.doi.org/10.1177/1461444816639975.

Hong Y., Harwit E. (2020). China's Globalizing Internet: History, Power, and Governance. *Chinese Journal of Communication*, vol. 13, iss. 1, pp. 1–7. https://doi.org/10.1080/17544750.2020.1722903.

Huawei (n. d.) Available at: https://www.huawei.com (accessed 6 April 2021).

Internet Assigned Numbers Authority (IANA) (n. d.). List of Root Servers. Available at: https://www.iana.org/domains/root/servers (accessed 6 April 2021).

Internet Corporation for Assigned Names and Numbers (ICAAN) (2016). NTIA IANA Functions' Stewardship Transition. Available at: https://www.icann.org/stewardship (accessed 6 April 2021).

Internet Corporation for Assigned Names and Numbers (ICAAN) (n. d., a). List of Accredited Registrars. Available at: https://www.icann.org/en/accredited-registrars?filter-letter=a&sort-direction=desc&sort-param=name&page=1 (accessed 6 April 2021).

Internet Corporation for Assigned Names and Numbers (ICAAN) (n. d., b). GAC Membership. Available at: https://gac.icann.org/about/members# (accessed 6 April 2021).

Internet Corporation for Assigned Names and Numbers (ICAAN) (n. d., c.). Root Server System Advisory Committee. Available at: https://www.icann.org/groups/rssac (accessed 6 April 2021).

International Telecommunication Union (ITU) (n. d.). China. Available at: https://www.itu.int/online/mm/scripts/gensel9?_ctryid=1000100502 (accessed 6 April 2021).

Jakushev M. (2016). Itogi vsemirnoy vstrechi na vysshem urovne po voprosam informatsionnogo obshchestva [Results of the World High-Level Meeting on the Information Society]. *Pul's Kibermira*, vol. 19, no 1. Avail-

able at: http://www.pircenter.org/articles/2009-itogi-vsemirnoj-vstrechi-na-vysshem-urovne-po-voprosam-informacionnogo-obschestva (accessed 6 April 2021). (In Russian)

Jiang M. (2010). Authoritarian Informationalism: China's Approach to Internet Sovereignty. *SAIS Review of International Affairs*, vol. 30, no 2, pp. 71–89. http://dx.doi.org/10.1353/sais.2010.0006.

Kleinwächter W. (ed.) (2007). *The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment*. Berlin: Marketing für Deutschland.

Larionova M., Shelepov A. (2021). Formirujushhiesja mehanizmy regulirovanija cifrovoj jekonomiki. Riski i vozmozhnosti dlja mnogostoronnej sistemy globalnogo upravlenija [Emerging Regulation for the Digital Economy: Challenges and Opportunities for Multilateral Global Governance]. *International Organisations Research Journal*, vol. 16, no 1, pp. 29–63. https://doi.org/10.17323/1996-7845-2021-01-02.

Li C., Li H. (2018). Global Governance of the Internet Based on Sovereignty in Cyberspace. *E-Government*, vol. 185, no 5, pp. 9–17. (In Chinese)

Li H. (2020). "Digital Silk Road" and the Reconstruction of Global Cyberspace Governance. *International Forum*, vol. 21, no 6, pp. 42–4. (In Chinese)

Li Z., Tang R. (2020). Multi-Stakeholder Model: Path to Build Global Internet Governance System. *Media Observer*, vol. 444, no 12, pp. 21–8. (In Chinese)

Michalopoulos S. (2019). Huawei Official: 5G Is a "Historic" Opportunity for Greece and Cyprus. Euroactiv, 30 July. Available at: https://www.euractiv.com/section/5g/news/huawei-official-5g-is-a-historic-opportunity-for-greece-and-cyprus/ (accessed 6 April 2021).

Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Minkomsvyaz Russia) (2017). Kontseptsiya konventsii OON (ili kontseptsiya bezopasnogo funktsionirovaniya i razvitiya seti Internet) [The Concept of Safe Functioning and Development of the Internet]. Available at: https://digital.gov.ru/uploaded/files/prilozheniekontseptsiikonventsiioon.docx (accessed 6 April 2021). (In Russian)

Ministry of Foreign Affairs of People's Republic of China (PRC) (2017). International Strategy of Cooperation on Cyberspace. Available at: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml (accessed 6 April 2021).

Ministry of Foreign Affairs of the Russian Federation (MFA Russia) (2009). Mnogostoronniye dogovory [Multilateral Agreements]. Available at: https://www.mid.ru/ru/foreign_policy/international_contracts/multilateral_contract/-/storage-viewer/multilateral/page-1/50243 (accessed 6 April 2021). (In Russian).

Ministry of Foreign Affairs of the Russian Federation (MFA Russia) (2011). Konventsiya ob obespechenii mezhdunarodnoy informatsionnoy bezopasnosti (kontseptsiya) [Convention on International Information Security]. 22 September. Available at: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (accessed 6 April 2021). (In Russian)

Moore M. (2016). Tech Giants and Civic Power. Centre for the Study of Media, Communication & Power, King's College London. Retrieved February, vol. 5, pp. 88. Available at: https://www.kcl.ac.uk/policy-institute/assets/cmcp/tech-giants-and-civic-power.pdf (accessed 19 August 2021).

Mueller M.L. (2020). Against Sovereignty in Cyberspace. *International Studies Review*, vol. 22, iss. 4, pp. 779–801. https://doi.org/10.1093/isr/viz044.

Negro G. (2020). A History of Chinese Global Internet Governance and Its Relations With ITU and ICANN. *Chinese Journal of Communication*, vol. 13, iss. 1, pp. 104–21. https://doi.org/10.1080/17544750.2019.1650789.

NETmundial (2014). Multistakeholder Statement. The Global Multistakeholder Meeting on the Future of Internet Governance. Available at: https://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (accessed 6 April 2021).

National Telecommunications and Information Administration (NTIA) (1998). Statement of Policy on the Management of Internet Names and Addresses. 5 June. Available at: https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses (accessed 6 April 2021).

Nokia (n. d.) Available at: https://www.nokia.com (accessed 6 April 2021).

Nye J.S. (2020). Power and Interdependence With China. *The Washington Quarterly*, vol. 43, iss. 1, pp. 7–21. https://doi.org/10.1080/0163660X.2020.1734303.

Organski A.F.K. (1958). *World Politics*. New York: A. Knopf.

Organski A.F.K., Kugler J. (1980). *The War Ledger*. Chicago: The University of Chicago Press.

People's Republic of China (PRC) (2010). White Paper on the Internet in China. Available at: https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm (accessed 6 April 2021).

Ponka T., Ramich M., Yu U. (2020). Informatsionnaya politika i informatsionnaya bezopasnost' KNR:razvitiye, podkhody i realizatsiya [Information Policy and Information Security of PRC: Development, Approaches and Implementation]. *Vestnik RUDN: International Relations*, vol. 20, no 2, pp. 382–94. https://doi.org/10.22363/2313-0660-2020-20-2-382-394.

Shen H. (2016). China and Global Internet Governance: Toward an Alternative Analytical Framework. *Chinese Journal of Communication*, vol. 9, iss. 3, pp. 304–24. Available at: https://doi.org/10.1080/17544750.2016.1206028

Slaughter A.M. (2009). America's Edge: Power in the Networked Century. *Foreign Affairs*, vol. 88, no 1, pp. 94–113. Available at https://www.jstor.org/stable/20699436 (accessed 6 April 2021).

Strickling L.E., Hill J.F. (2017). Multi-Stakeholder Internet Governance: Successes and Opportunities. *Journal of Cyber Policy*, vol. 2, iss. 3, pp. 296–317. https://doi.org/10.1080/23738871.2017.1404619.

Suvorov A. (2020). Sovremennye realii kiberprostranstva: Rossija kak vedushhij igrok v obespechenii mezhdunarodnoj informacionnoj bezopasnosti [The Present Realities of Cyberspace: Russia as a Leading Player in International Information Security]. PIR-Centre, 2 November. Available at: http://www.pircenter.org/blog/view/id/433 (accessed 6 April 2021). (In Russian)

The White House (2011). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed 6 April 2021).

United Nations (UN) (2003). Deklaratsiya printsipov. Postroyeniye informatsionnogo obshchestva – global'naya zadacha v novom tysyacheletii: Vsemirnaya vstrecha na vysshem urovne po voprosam informatsionnogo obshchestva. Zheneva, 2003 g. Tunis, 2005 g. [Declaration of Principles: Building the Information Society: A Global Challenge in the New Millennium. World Summit on the Information Society. Geneva, 2003–Tunis, 2005]. Available at: https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (accessed 6 April 2021). (In Russian)

United Nations (UN) (2005). Tunisskaya programma dlya informatsionnogo obshchestva: Vsemirnaya vstrecha na vysshem urovne po voprosam informatsionnogo obshchestva. Zheneva, 2003 g.–Tunis, 2005 g [Tunis Agenda for the Information Society. World Summit on the Information Society. Geneva, 2003–Tunis, 2005]. Available at: https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (accessed 6 April 2021). (In Russian).

United States Congress (2012). International Proposals to Regulate the Internet. Committee on Energy and Commerce, 31 May. Available at: https://archive.org/details/gov.gpo.fdsys.CHRG-112hhrg79558/page/n11/mode/2up (accessed 6 April 2021).

United States Department of Defense (2018). Summary: Department of Defense Cyber Strategy. Available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed 6 April 2021).

United States Department of Defense (2021). List of Additional Companies, in Accordance With Section 1237 of FY99 NDAA. News Release, 14 January. Available at: https://www.defense.gov/Newsroom/Releases/Release/Article/2472464/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/ (accessed 6 April 2021).

United States Department of State (n. d.). The Clean Network. Available at: https://2017-2021.state.gov/the-clean-network/index.html (accessed 6 April 2021).

van Eeten M.J.G., Mueller M. (2013). Where Is the Governance in Internet Governance? *New Media & Society*, vol. 15, iss. 5, pp. 720–36. https://doi.org/10.1177%2F1461444812462850.

Vasilkovsky S., Ignatov A. (2020). Upravlenie Internetom: sistemnye disproporcii i puti ih razreshenija [Internet Governance: System Imbalances and Ways to Resolve Them]. *International Organisations Research Journal*, vol. 15, no 4, pp. 7–29. https://doi.org/10.17323/1996-7845-2020-04-01.

Wang Z. (2020). The New Dynamics of Global Cyberspace Rule-Making Under the UN Dual-Track System. *China Information Security*, vol. 20, no 1, pp. 40–3. (In Chinese)

World Internet Conference (WIC) (2020). Initiative on Jointly Building a Community With a Shared Future in Cyberspace. News, 18 November. Available at: http://www.wuzhenwic.org/2020-11/18/c_564467.htm (accessed 6 April 2021).

Xiaomi (2021). Statement. 14 March. Available at: https://blog.mi.com/en/2021/03/14/statement/ (accessed 6 April 2021).

Xu P. (2021). 2020 Global Internet Governance Towards Digital Cold War or Digital Commons. *Information Security and Communications Privacy*, vol. 21, no 3, pp. 16–23. (In Chinese)

Yan L. (2019). Global Cyberspace Governance: State Actors and the China-US Cyber Relationship. *Contemporary International Relations*, vol. 29, no 2, pp. 105–24. Available at: http://www.cicir.ac.cn/UpFiles/file/20200227/637184169973143065186752 2.pdf (accessed 19 August 2021).

Yang G. (2014). The Return of Ideology and the Future of Chinese Internet Policy. *Critical Studies in Media Communication*, vol. 31, iss. 2, pp. 109–13. https://doi.org/10.1080/15295036.2014.913803.

Zeng J., Stevens T., Chen Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty." *Politics & Policy*, vol. 45, issue 3, pp. 432–64. https://doi.org/10.1111/polp.12202.

Zhao R. (2021). Global Network Governance Reform: Path Choices for Rising Powers. *Academia*, vol. 272, no 1, p. 50–9. (In Chinese)

Zhu D., Liu Y-W. (2021). The Legal Governance System of Cyberspace in the Community of Shared Future of Mankind and China's Plans. *Journal of Yangtze Normal University*, vol. 37, no 1, pp. 30–9. (In Chinese)

Zinovieva E. (2015). Globalnoe upravlenie Internetom: rossijskij podhod i mezhdunarodnaja praktika [Global Internet Governance: Russian Approach and International Practice]. *MGIMO Review of International Relations*, vol. 43, no 4, pp. 111–8. https://doi.org/10.24833/2071-8160-2015-4-43-111-118.

ZTE (n. d.). Available at: https://www.zte.com.cn/ (accessed 6 April 2021).