

ИСТОРИЯ РАЗВИТИЯ КИБЕРДИПЛОМАТИИ КИТАЯ: 1994-2023 ГГ.

Куликов Денис Алексеевич

Аспирант, Санкт-Петербургский
государственный университет
denisk7873@gmail.com

THE HISTORY OF THE DEVELOPMENT OF CHINESE CYBER DIPLOMACY: 1994-2023

D. Kulikov

Summary: Cyber diplomacy in the context of digitalization of most processes has long been an important aspect of international relations, and one of the most influential states participating in this process at the present stage is China. The evolution of the cyber diplomacy of this state is a unique phenomenon reflecting the technological changes that have occurred in China over the past two decades. The transformation of many public diplomacy processes towards digital diplomacy, datification and new approaches to big data analysis have led to a change in China's foreign policy strategies.

In the context of a new round of struggle for global leadership between developed powers, an increase in the number of cyber attacks and the presence of many territorial conflicts, China's role in using cyber diplomacy is of particular importance.

The author's goal was to analyze the retrospective of the development of cyberdiplomacy in China, as well as to identify the key stages of this evolution.

Keywords: cyberdiplomacy, history of cyberdiplomacy, China, cybersecurity, information security, digital diplomacy, data diplomacy, technology, foreign policy strategies.

Аннотация: Кибердипломатия в условиях цифровизации большинства процессов уже давно стала важным аспектом международных отношений, и одним из наиболее влиятельных государств-участников этого процесса на современном этапе является Китай. Эволюция кибердипломатии данного государства представляет собой уникальное явление, отражающее технологические изменения, произошедшие в Китае на протяжении двух последних десятилетий. Трансформация многих процессов публичной дипломатии в сторону цифровой дипломатии, датификация и новые подходы к анализу больших данных привели к изменению внешнеполитических стратегий Китая.

В условиях нового витка борьбы за глобальное лидерство между развитыми державами, роста числа кибератак и наличия множества территориальных конфликтов, роль Китая в использовании кибердипломатии приобретает особое значение.

Перед автором стояла цель проанализировать ретроспективу развития кибердипломатии в Китае, а также выявить ключевые этапы этой эволюции.

Ключевые слова: кибердипломатия, история кибердипломатии, Китай, кибербезопасность, информационная безопасность, цифровая дипломатия, дипломатия данных, технологии, внешнеполитические стратегии.

Возникновение суверенного цифрового пространства. 1994-2009 гг.

В 1994 году доступ к интернету был открыт для первых китайских пользователей. Коммунистическое руководство пошло на этот шаг для притока свежей мысли и научных знаний. Однако, несмотря на это, вплоть до 2010-х годов основным вектором развития китайского общества был курс на суверенизацию цифрового пространства и информационную изоляцию.

Данный период времени характеризовался стремлением Китая сегментировать глобальный интернет, огородить и защитить свою региональную зону от внешнего воздействия. Для этих целей были использованы «жесткие методы» цифровой политики.

К примеру, в 1998 году была создана система интернет-безопасности Золотой Щит (Великий китайский файрволл) [1]. Ее основными задачами были сквозная идентификация пользователей (авторизация по паспортным данным), мониторинг кибератак, логирова-

ние трафика, фильтрация контента, видеомониторинг и антивирусные системы. Однако, помимо стандартного функционала, система содержала в себе прорывные на тот момент особенности: возможность распознавания лиц и определение местонахождения нарушающих закон пользователей.

Но, помимо этого, применялись и инструменты «мягкой силы». Велась подготовка квалифицированных кадров для работы на укрепление защиты стратегической инфраструктуры, вносились поправки в национальное законодательство КНР, проводилась линейная пропаганда о нежелательности использования глобального интернета, укреплялась система обеспечения технологической и информационной безопасности.

Первым шагом в развитии кибердипломатии Китая стало подписание в 2006 году Заявления глав-государств ШОС по международной информационной безопасности [2]. На совместной встрече представителей блока государств обсуждались вопросы информационной безопасности как важного фактора обеспечения нацио-

нальной стабильности и государственного суверенитета.

К концу 2010-х годов доступ ко Всемирной сети был лишь у половины населения Китая [3]. Но именно в этот период была заложена база для создания автономного национального интернет-пространства со всем необходимым для жизни и работы программным обеспечением. Такая стратегия позволила Китаю не чувствовать зависимости от западных технологий и продолжить развивать свою суверенную политику кибердипломатии.

Параллельно в 2007 году начались первые обсуждения основных принципов «мягкой силы» с «китайской спецификой» [4]. Ху Цзинтао отмечал, что неклассические инструменты внешнеполитической деятельности также важны для страны, как и прежние традиционные методы.

Начало международного сотрудничества. 2010-2018 гг.

В 2010 году в документах Государственного совета впервые упоминается слово «киберсуверенитет» или «сетевой суверенитет» [5]. Государство официально признало Интернет частью национальной инфраструктуры. Таким образом, начинает расти число пользователей, увеличиваются охваты и масштаб использования цифровых технологий. Что, в свою очередь, требовало юридического закрепления понятий в новой концепции развития Китая.

В 2011 году при участии китайской делегации было подписано Соглашение между государствами-членами ШОС о сотрудничестве в области международной информационной безопасности [6].

Таким образом, фрагментация интернета перестала носить абсолютный характер и китайское руководство решило осуществлять первые шаги по налаживанию международного сотрудничества в сфере управления глобальным интернетом.

Постепенно начинает формироваться вектор на развитие цифровой дипломатии. На первый план выходят задачи по продвижению позитивного имиджа государства, а также распространению китайских ценностей и культуры за рубежом. В 2013 году Си Цзиньпин впервые высказался относительно важности использования публичной дипломатии для современного Китая. Лидер заявил о том, что новые методы цифровой дипломатии позволят эффективнее продвигать политические задачи Китая на мировой арене, а также реализовывать идею «китайской мечты» [7].

Стоит отметить, что подход Китая к использованию

цифровой дипломатии сильно отличается от практики других развитых стран. Дело в том, что Китай выступает против унификации стандартов и использует возможности глобализации для культурной экспансии. С учетом общего упора на китайскую традиционную культуру и наличия центрального государственного планирования, цифровая дипломатия Китая сильно выделяется среди конкурентов на мировой арене.

В 2014 году в рамках первой Всемирной интернет-конференции Генеральный секретарь Си Цзиньпин впервые официально объявил миру о китайском видении концепции киберсуверенитета [8]. Основные тезисы были закреплены в том же году в Китайской декларации по Интернету [9], а также в Проекте Декларации Учжэнь [10].

С точки зрения китайского руководства, новые технологии бросают вызов суверенитету государства, что требует создания совместных систем сетевой безопасности. Поскольку мероприятие имело международный статус, а в качестве приглашенных лиц были крупные транснациональные корпорации и иностранные делегаты разных стран, Китай планировал использовать эту возможность для продвижения нескольких инициатив в международном законодательстве, выгодных китайскому правительству.

По ряду причин попытка оказалась неудачной. Однако, на фоне волны обвинений Китая в кибератаках, кибершпионаже и краже американских данных, во время второй Всемирной интернет-конференции в 2015 году внимание Китая было сосредоточено уже на проблемах развивающихся стран и попытке укрепить международное сотрудничество с Россией в сфере кибербезопасности.

Итогом переговоров между делегациями с участием российской «Лаборатории Касперского» и китайской Zhongguo Wangan стало подписание Соглашения между правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности [11].

На фоне отсутствия сотрудничества со странами запада, преобладания американской кибергегемонии и растущего цифрового неравенства стороны договора признавали принцип суверенного равенства в киберпространстве, а также право наций самостоятельно управлять этой сферой.

Также Китай расширил сферу государственного управления, добавив киберпространство в качестве новой государственной границы в дополнение к имеющимся у государства морской, сухопутной, воздушной и

космической [12]. Эта идея нашла отклик и у российской стороны, поскольку оба государства сделали акцент на киберсуверенитете и национальной безопасности.

Позднее эти принципы еще не раз озвучивались в рамках Афро-азиатской консультативно-правовой организации в 2014 году [13], Международного симпозиума по кибербезопасности в 2016 году [14], а также были закреплены в Декларации Гоа 2016 года [15], Международной стратегии взаимодействия в киберпространстве 2017 года [16] и Циндаоской декларации Совета глав государств-членов Шанхайской организации сотрудничества 2018 года [17].

В документах также содержались призывы к продвижению совместных идей через существующие диалоговые площадки (ICANN, Всемирный экономический форум, Форум по вопросам управления Интернетом и т.д.), а также через создание альтернативных площадок для помощи развивающимся странам на базе стран ШОС, АСЕАН и БРИКС. Основной причиной подобной инициативы стал усугублявшийся раскол между странами. США и государства западного блока критиковали идеи Китая, поскольку опасались влияния авторитарных режимов и их идей на киберпространство [18].

Таким образом, Китай продолжил укреплять свое сотрудничество с развивающимися странами в рамках новых проектов и международных организаций. К примеру, в 2015 году была создана стратегическая инициатива «Цифровой шелковый путь», основной целью которой был поиск новых рынков в развивающихся странах для размещения хайтек-компаний, а также реализации совместных технологических проектов [19]. В 2017 году была выдвинута и одобрена инициатива создания Института БРИКС по изучению сетей будущего – «BRICS Future» [20]. Его основной целью стало развитие программ искусственного интеллекта, построение новых безопасных сетевых платформ и дальнейшее развитие международного сотрудничества.

К концу второго десятилетия XXI века Китай и Россия уже активно занимались разработкой инфраструктуры 5G и обсуждали совместную разработку технологий Интернета вещей (IoT), а инвестиции в технологические проекты российских компаний достигли 100 млн долларов [21].

Современная кибердипломатия. 2019–2025 гг.

В рамках шестой (2019 год), седьмой (2020 год) и восьмой (2021 год) Всемирных интернет-конференций Китай окончательно утвердил киберсуверенитет в качестве фундаментального принципа построения кибердипломатии. Регулирование цифрового пространства признается естественным, равным и неотчуждаемым правом

каждого государства в отдельности.

Вместе с тем Китай не отказывается от возможности создания глобальной системы кибербезопасности общими усилиями. В частности, государством предлагается усиливать международное законодательство в киберпространстве и создавать новые мозговые центры по изучению технологий.

Одним из примеров успешного сотрудничества стало открытие в 2019 году Китайско-израильского центра инновационных технологий в области информационной безопасности, а также индустриального парка совместных технологий Китая и Израиля [22].

Наступает эпоха расцвета цифровой дипломатии, к которому Китай подтолкнули два события: резкий скачок технологического прогресса и открытая критика американских властей по нескольким вопросам, включая распространение COVID-19.

В 2019 году представители дипломатических ведомств КНР регистрируют свои первые официальные аккаунты в социальных сетях. Выделяется два основных сегмента аудитории. К первому сегменту были отнесены жители китайских диаспор, Гонконга и Тайваня. Ко второму сегменту представляющие интерес иностранные граждане (туристы, бизнесмены и молодежь ближнего зарубежья).

Распространению нужной информации способствуют другие каналы коммуникации, в частности, специализированные китайские цифровые издания (China Daily, Global Times), китайские социальные сети и сервисы (Sina Weibo, RenRen, WeChat, TikTok, QQ), а также блокировка популярных западных сервисов (Twitter, Facebook, Instagram) в периоды обострения обстановки в КНР. Доступность китайских сервисов более чем на 15 различных языках, а также наличие 50-миллионной армии мигрантов (хуацяо) способствует дополнительному продвижению необходимых Китаю идей на мировой арене. Одним из наиболее значимых достижений цифровой дипломатии Китая является переориентация мышления у хуацяо: если раньше они считали своей родиной Китайскую Республику (г. Тайбэй), то теперь их родина – КНР [23].

В то же время политическое руководство Китая начинает сталкиваться с рядом новых проблем в цифровом пространстве. Появление возможности быстрого создания, распространения и фильтрации контента в Интернете самими пользователями сильно затруднило агитацию и пропаганду среди целевой аудитории. Наглядным примером эффективной скоординированной работы через социальные сети стала подготовка протестов в Гонконге в 2019–2020 годах.

Для решения подобных проблем в стране уже создано несколько центров по подготовке «кибер-солдат» с общей численностью более 300 тысяч человек, основной целью которых является размещение необходимой информации на форумах, сайтах и в блогах, удаление постов, отключение функционала комментариев и репостов под записями.

Внутри государства Китай осуществляет жесткое регулирование медиа, чтобы избежать политической дестабилизации, а в случае с иностранной аудиторией старается допускать некоторые послабления, развенчивая мифы о закрытости китайского общества.

Расширяется и международное нормативное законодательство. В 2020 году была запущена «Инициатива Китая и АСЕАН по созданию партнерства в области цифровой экономики» [24], в 2021 году принимаются «Инициатива по совместному созданию китайско-африканского сообщества единой судьбы в киберпространстве» [25] и «Китайско-арабская инициатива по сотрудничеству в области безопасности данных» [26], а в 2022 году публикуется совместная инициатива Китая, Казахстана, Таджикистана, Киргизии, Узбекистана и Туркменистана «Китай + пять стран Центральной Азии» [27].

Все перечисленные выше документы и инициативы

отражают современный взгляд Китая на сферу кибердипломатии, основой которой является уважение киберсуверенитета других стран.

Таким образом, политическое руководство страны придает особую важность обеспечению безопасности ключевой информационной инфраструктуры глобальной сети, одновременно стремясь снизить технологическую зависимость от западных стран. Достичь этих целей Китай планирует путем внедрения собственных инноваций и создания конкуренции для зарубежных компаний на новых рынках развивающихся стран. В дополнение к этому также планируется увеличение расходов на кибербезопасность до 22 млрд. долларов к 2025 году [28].

В целом можно отметить, что использование кибердипломатии позитивно сказывается на внешней политике Китая, увеличивая его международное влияние. Развитие цифровых технологий позволяет формировать положительный имидж государства на мировой арене и укреплять его положение как за рубежом, так и внутри страны. Использование ИКТ, методов цифровой дипломатии, анализа «больших данных» и наличие высококвалифицированных специалистов в области науки и техники позволяют прогнозировать поведение аудитории, а также оказывать необходимое воздействие для достижения поставленных целей.

ЛИТЕРАТУРА

1. Зиновьева Е.С. Кибер-дипломатия в условиях обострения конкуренции между великими державами // Вестник МГИМО-Университета. - М.: МГИМО МИД России, 2022. - С. 1.
2. Заявление глав государств-членов ШОС по международной информационной безопасности // Центральный интернет-портал Шанхайской организации сотрудничества URL: <http://www.infoshos.ru/ru/?id=94> (дата обращения: 03.03.2024).
3. Как развивался IT-сектор Китая и почему правительство страны объявило ему войну // Хабр URL: <https://habr.com/ru/companies/onlinepatent/articles/797247/> (дата обращения: 03.03.2024).
4. Подоляк Д.В. СМИ как инструмент «мягкой силы» во внешней политике КНР // Общество: политика, экономика, право. - 2018. - №11 (64).
5. White papers // The State Council of the People's Republic of China URL: <http://english.www.gov.cn/> (дата обращения: 02.03.2024).
6. Соглашение между правительствами государств-членов ШОС о сотрудничестве в области международной информационной безопасности // Электронный фонд правовой и нормативно-технической информации URL: <https://docs.cntd.ru/document/902289626> (дата обращения: 02.03.2024).
7. Инь Сымэн, Цветкова Н.А. Место и роль личного образа Си Цзиньпина в публичной дипломатии Китая // Дипломатическая служба. 2018. №4. С. 44-48.
8. Си Цзиньпин призывает создать в киберпространстве сообщество с единой судьбой // ИА Синьхуа URL: https://russian.news.cn/2015-12/16/c_134922755.html (дата обращения: 02.03.2024).
9. China Delivers Midnight Internet Declaration // The Wall Street Journal URL: <https://www.wsj.com/articles/BL-CJB-24963> (дата обращения: 02.03.2024).
10. Декларация Учжэнь // ИА Синьхуа URL: <http://www.xinhuanet.com/politics/2015> (дата обращения: 02.03.2024).
11. Соглашение от 30 апреля 2015 г. между правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности // Электронный фонд правовой и нормативно-технической документации URL: <https://docs.cntd.ru/document/420271846> (дата обращения: 03.03.2024).
12. Янькова А.Д. Архитектура концепции киберсуверенитета КНР (по материалам докладов Всемирной интернет-конференции «Киберсуверенитет: теория и практика») // Проблемы Дальнего Востока. - 2023. - №4. - С. 4.
13. Conferences // Asian African Legal Consultative Organization URL: <https://aalco.int/> (дата обращения: 01.03.2024).
14. International Workshop on Cyber Security // Ministry of Foreign Affairs of the People's Republic of China URL: https://www.fmprc.gov.cn/web/wjb_673085/zjg_673183/jks_674633/jksxwlb_674635/201607/t20160711_7666933.shtml (дата обращения: 04.03.2024).
15. Киберсуверенитет: теория и практика // 安全内参 URL: <https://www.secrss.com/articles/27378> (дата обращения: 04.03.2024).

16. International Strategy of Cooperation on Cyberspace // China Media URL: <https://chinacopyrightandmedia.wordpress.com/2017/03/01/international-strategy-of-cooperation-on-cyberspace/> (дата обращения: 04.03.2024).
17. Циндаоская декларация Совета глав государств-членов Шанхайской организации сотрудничества // Сайт Президента России URL: <http://www.kremlin.ru/supplement/5315> (дата обращения: 04.03.2024).
18. Hitchens T., Goren N. International Cybersecurity Information Sharing Agreements. Maryland: Center for International & Security Studies, 2017. P.44.
19. Jing Chenga, Jinghan Zeng "Digital Silk Road" as a Slogan Instead of a Grand Strategy // Journal of Contemporary China. 2023. Vol. 32. No. 142. P. 2.
20. Институт БРИКС по изучению сетей будущего открыл филиал в городе Шэньчжэнь // Национальный комитет по исследованию БРИКС, Россия URL: <https://nkibrics.ru/posts/show/5d4d3ba6627269166c0b0000> (дата обращения: 04.03.2024).
21. Гусевская А.А. Цифровая дипломатия Китая: укрепление связей с Россией с помощью технологий // Россия - Китай: развитие регионального сотрудничества в XXI веке. Материалы XXI Международной научно-практической конференции. - Чита: Забайкальский государственный университет, 2023. - С. 47.
22. Официальный сайт центра информационной безопасности «360» URL: <https://www.360.cn>. (дата обращения: 04.03.2024).
23. Аликберова А.Р., Балакин Д.А. Цифровая дипломатия с китайской спецификой // Modern Oriental Studies. 2019. № 3. С. 79.
24. Китай и АСЕАН намерены развивать сотрудничество в области цифровой экономики. URL: <https://news.rambler.ru/asia/44339969-kitay-i-asean-namereny-v-2020-godu-razvivat-sotrudnichestvo-v-oblasti-tsifrovoy-ekonomiki/> (дата обращения: 05.03.2024).
25. Резюме Китайско африканского форума по развитию и с о трудничеству в Интернете // РИА Новости URL: <https://ria.ru/20211207/investitsii-1762532674.html> (дата обращения: 05.03.2024).
26. Китайско-арабская инициатива по сотрудничеству в области безопасности данных // Портал законов Китая URL: <https://ru.chinajusticeobserver.com/law/x/global-initiative-on-data-security-2020098> (дата обращения: 05.03.2024).
27. Китай плюс пять: В Азии рождается новый механизм сотрудничества // Российская газета URL: <https://rg.ru/2023/05/18/kitaj-plus-piat.html> (дата обращения: 05.03.2024).
28. Правительство Китая усилит кибербезопасность страны // Cyber Media URL: <https://securitymedia.org/news/pravitelstvo-kitaya-usilit-kiberbezopasnost-strany.html> (дата обращения: 05.03.2024).

© Куликов Денис Алексеевич (denisk7873@gmail.com).

Журнал «Современная наука: актуальные проблемы теории и практики»