

ЦИФРОВЫЕ СТРАТЕГИИ КАК ИНСТРУМЕНТ В БОЛЬШОЙ ПОЛИТИЧЕСКОЙ ИГРЕ.

Захарова А.В. (Санкт-Петербургский государственный университет), **Крикухин И.Ю.**
(Санкт-Петербургский государственный экономический университет)

Научный руководитель – доцент, кандидат политических наук Ковалевская Н.В.
(Санкт-Петербургский государственный университет)

Введение. В настоящее время цифровизация является глобальной вехой развития общества. Государства фигурируют в качестве глобальных игроков на просторах Сети, что приводит к столкновениям интересов, различным формам давления на оппонента и «территориальным» спорам. Это создает необходимость выработать чёткие стратегии для защиты и продвижения собственных интересов. Данное исследование описывает различные подходы к внедрению технологий в цифровое пространство отдельных государств, а также позволяет провести сравнительный анализ применения различных стратегий и методов внутренней политики разных стран в киберпространстве на примере США и КНР. Планируется провести сравнительный анализ для ответа на вопрос: почему, несмотря на различный культурный код цитаделей развития технологий в разных точках земного шара, государства, при внедрении технологий в жизнь граждан и ведении идеологического противостояния, преследуют похожие цели?

Основная часть. Во внутренней политике США и Китай действуют по схожим паттернам, а разница методов воздействия заключается лишь в форсированном внедрении и радикальности подхода государственных структур к общественной и частной жизни отдельно взятого гражданина. В сравнении с азиатским подходом, западные методы представляются внешне более демократическими, однако при более детальном рассмотрении представляют собой схожий паттерн поведения. Помимо этого, цифровые стратегии США и Китая в 21 веке отличаются по нескольким параметрам, и есть несколько предметных областей для сравнения, которые позволят сделать сравнительный анализ более точным:

1. Подход к критической информационной инфраструктуре: обе страны уделяют значительное внимание развитию цифровизации: США сосредоточены на развитии сетей 5G, высокоскоростной широкополосной связи и расширении доступа к высокоскоростному интернету по всей стране. Китай, напротив, уделяет большое внимание созданию национальной высокоскоростной интернет-магистральной и продвижению использования искусственного интеллекта в ряде отраслей, в частности, в сфере национальной безопасности, контроля граждан и области стратегических вооружений.

2. Подход к кибербезопасности: обе страны уделяют значительное внимание кибербезопасности, при этом США сосредоточены на защите критической инфраструктуры и создании системы международных норм, которая позволила бы сформировать стратегическую коалицию по контролю всему мировому Интернету, в то время как Китай делает упор на развитие системы защиты национального Интернета, промышленный шпионаж, создание независимой критической информационной инфраструктуры, а также развитие своих оборонительных и наступательных возможностей в киберпространстве.

3. Наступательные возможности: США публично заявили, что они оставляют за собой право использовать наступательные кибер-операции в ответ на кибератаки или угрозы национальной безопасности. Китай не делал подобных заявлений, однако обвиняется Штатами в проведении кибератак, включая шпионаж, кражу интеллектуальной собственности и использование средств для манипулирования иностранными выборами и общественным мнением.

4. Подход к конфиденциальности и контролю трафика: США уделяют большое внимание формированию образа «свободного Интернета», где провозглашаются ценности по защите частной жизни и существует целый ряд законов по защите персональных данных. Несмотря на это, в США активно применяется система мониторинга местонахождения пользователей и

отслеживания их информационного портрета, в частности, корпорацией Meta и спецслужбами ЦРУ. В отличие от политики формирования имиджа демократической страны, Китай не стремится экспортировать имидж «свободного Интернета» и внедряет всеобъемлющую систему социального кредитования, которая отслеживает поведение граждан и использует искусственный интеллект для наблюдения и контроля за населением. Используя технологии распознавания лиц и другие инновации, осуждаемые западным сообществом, Китай не скрывает намерений создать безопасную и подконтрольную партии Сеть, где цифровой портрет каждого гражданина будет отражаться на его социальном рейтинге.

5. Подход к глобальному влиянию: США являются главным сторонником открытого и свободного интернета, экспортируя демократические ценности и образ «свободной страны», внедряя технологии слежения и стремясь сформировать такую стратегическую коалицию, которая позволила бы монополизировать мировой Интернет и вводить единые нормы контроля трафика. В отличие от западной парадигмы развития, Китай сосредоточен на создании собственных глобальных технологических компаний и продвижении более закрытой, контролируемой государством модели интернета.

Выводы. И США, и Китай инвестируют значительные средства в развивающиеся технологии, такие как 5G, искусственный интеллект и квантовые вычисления, которые могут иметь значительные последствия для кибербезопасности и национальной безопасности стран по всему миру. Поскольку эти технологии продолжают развиваться, вполне вероятно, что обе страны будут стремиться установить доминирование в этих областях, что сформирует биполярную геополитическую систему, характеризующуюся стратегическим соперничеством в области передовых технологий. Глобальная геополитическая напряженность между США и Китаем по таким вопросам, как торговля, права человека и раздел сфер влияния может перейти в область киберпространства. Несмотря на то, что и США, и Китай являются друг для друга крупнейшими экономическими партнерами в вопросах экспорта высоких технологий, а также призывают к международному сотрудничеству в области кибербезопасности, реальность такова, что обе страны предпринимают действия, нацеленные на формирование несбалансированной, центричной системы, в которой соперничество и взаимные угрозы станут реалиями современности, в которой будет невозможно обеспечить глобальную кибербезопасность. Вероятно, что США и Китай останутся основными игроками в киберпространстве, а конкуренция между этими двумя странами будет оставаться главной причиной напряженности и беспокойства.

Список использованных источников:

1. Anton Dengg, Michael Schurian (Eds.), On the Concept of Hybrid Threats. In: DENG G, Anton, ed., Michael SCHURIAN, ed. Networked Insecurity: Hybrid Threats in the 21st Century. Wien: Landesverteidigungsakademie, 2017, 25-80.

2. Цифровая трансформация отраслей: стартовые условия и приоритеты: докл. к XXII Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 13–30 апр. 2021 г. / Г. И. Абдрахманова, К. Б. Быховский, Н. Н. Веселитская, К. О. Вишневецкий, Л. М. Гохберг и др. ; рук. авт. кол. П. Б. Рудник ; науч. ред. Л. М. Гохберг, П. Б. Рудник, К. О. Вишневецкий, Т. С. Зинина ; Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2021. — 56.