

Н. А. Цветкова

ЦИФРОВЫЕ ИНСТРУМЕНТЫ В МЕЖДУНАРОДНОЙ ПОЛИТИКЕ: СОДЕРЖАНИЕ И МЕТОДЫ АНАЛИЗА

*Рекомендовано в качестве учебного пособия для студентов
высших учебных заведений, обучающихся по направлению
подготовки «Международные отношения»*



Санкт-Петербург
2023

УДК 327
ББК 66.4
Ц27

*Печатается по решению
кафедры американских исследований
Санкт-Петербургского государственного университета*

Цветкова Н. А.

Ц27 Цифровые инструменты в международной политике: содержание и методы анализа. Учебное пособие. — СПб.: Издательство Скифия-принт, 2023. — 56 с.

Учебное пособие направлено на формирование у студентов научных знаний о новом этапе развития системы международных отношений в цифровую эпоху.

В пособии раскрываются понятийный аппарат, научные концепции, методы анализа, а также компоненты цифровых международных отношений.

Учебное пособие сопровождается вопросами и аналитическими заданиями для повторения материала по курсу лекций *Цифровизация международных отношений*.

Пособие предназначено для обучающихся по направлению «Международные отношения».

УДК 327
ББК 66.4

ISBN 978-5-00197-086-6

© Н. А. Цветкова, 2023

СОДЕРЖАНИЕ

Введение	4
Раздел 1. Понятийный аппарат	5
Вопросы и аналитические задания	11
Рекомендованная литература	12
Раздел 2. Кластеры в цифровых международных отношениях ..	13
Примечания	17
Вопросы и аналитические задания	18
Рекомендуемая литература	18
Раздел 3. Механизм и особенности развития цифровых международных отношений	19
Вопросы и аналитические задания	32
Рекомендуемая литература	33
Раздел 4. Методы анализа цифровых международных отношений	34
Вопросы и аналитические задания	51
Рекомендованная литература	52
Темы для семинарских занятий	53
Рекомендуемая литература	54

Введение

Современные международные отношения — это не только противостояние различных ценностей, политических систем или экономик. Это противостояние различных реальностей, которые с информационными потоками из цифрового пространства переносятся в традиционные каналы и оказывают влияние на политическую стабильность в разных странах. Цифровизация раздробила международные отношения и дискурс о происходящих событиях на множество конкурирующих трактовок, интерпретаций, выраженных как в текстовом, так и в аудиовизуальном формате.

Стейкхолдеры (владельцы) созданных политических реальностей и информации в интернете оказывают влияние на восприятие мировой политики миллионами пассивных фолловеров. Многообразие пользователей в социальных сетях может ограничивать и расширять пространство для маневра государственной дипломатии. Ведущие государства и дипломаты воспользовались этой новой, раздробленной на фрагменты цифровой реальностью для решения своих внешнеполитических задач. Фрагментированная цифровая реальность позволяет цифровой дипломатии формировать представления о разных политических реальностях и сдерживать информационные кампании других государств или неправительственных акторов, продвигая собственную повестку, легитимируя собственные действия и делегитимируя действия противников. Эти особенности развития цифровых международных отношений требуют развернутой интерпретации на основе использования качественных и количественных методов анализа с включением анализа больших данных.

Поэтому цель данного учебного пособия — предоставить студентам фундаментальные и практические знания о системе цифровых международных отношений, в которых формируются новые альянсы участников мировой политики, выстраиваются линии противостояния и появляются точки турбулентности.

Пособие предназначено для студентов, обучающихся по направлению «Международные отношения» и изучающих дисциплины в области дипломатии данных, кибербезопасности, аналитики больших данных и публичной дипломатии.

Раздел 1

Понятийный аппарат

Международные отношения как система, включающая разнообразные элементы, отношения, дипломатию и пр., всё больше становится цифровой.

Цифровые международные отношения (cyber international relations) включают в себя кластеры как цифровая дипломатия, дипломатия данных; кибербезопасность и кибердипломатия; глобальное управление интернетом и цифровые избирательные технологии.

Цифровая дипломатия (digital diplomacy) — это взаимодействие правительств с пользователями социальных сетей для решения внешнеполитических задач. Существует разнообразие терминов. На заре институционализации данного дипломатического инструмента в 2010-е гг. первая серия терминов относительно использования цифровых технологий в политике состояла из таких понятий, как: «е-дипломатия», «программы web 2.0.», «интернет-дипломатия», «дипломатия социальных сетей или твипломаси». Это создавало неоднозначное понимание различных типов взаимодействий между дипломатией и миром цифровых технологий. В итоге термин *digital diplomacy* чаще использовался в официальных документах и самым точным образом описывал деятельность дипломатов в социальных сетях — формирование диалога с целевой аудиторией и использование цифровых инструментов в информационном противостоянии. В 2020-е гг. цифровая дипломатия опирается на алгоритмы и искусственный интеллект для расширения влияния государства, а также пересекается с вопросами кибербезопасности и кибердипломатии. Появилась дипломатия данных.

Большие данные и дипломатия данных — это правительственный механизм для решения задач информационного противостояния при помощи использования больших данных, ботов, искусственного интеллекта, что позволяет определять целевые аудитории, вычислять ключевых блогеров, а также эффективно разрабатывать контрмесседжи против пропаганды.

Глобальное управление интернетом — это комплекс проблем, процесс переговоров и соглашения между различными стейкхолдерами, включая государства и гражданское общество, по вопросам международного и суверенного контроля за киберпространством. Вопросы кибербезопасности и информационной безопасности также затрагиваются в данном курсе в рамках международной повестки.

Цифровые избирательные технологии являются бурно развивающейся областью международных отношений и подразумевают сравнительный анализ использования электронного или цифрового голосования в разных странах, а также затрагивают проблему влияния государств на политические процессы и выборы в зарубежных странах.

Современные международные отношения перешли в эпоху, когда взаимодействие между странами, прокси-группами или пользователями в киберпространстве необходимо регулировать цифровыми правилами либо в духе Ялтинских/Потсдамских соглашений и проведения красных линий в интернете, либо в стиле пунктов В. Вильсона об открытой дипломатии и, говоря современным языком, дипломатии и политики в прямом эфире.

Сформировалась та цифровая реальность, в которой большие данные и умелая аналитика «цифровых следов» оказывают влияние не только на пользователей социальных сетей — основных потребителей синтетической информации, — делая их заложниками эхо-камер, пузырей фильтров и фрагментированной политики, но и на основных акторов традиционной системы международных отношений — государства, — размывая силу и влияние на ход мировой политики. Разделяемый всё больше на национальные кластеры интернет, концентрация идеологий и ценностей в отдельных группах в социальных сетях и фильтрация информации по политическим предпочтениям создают условия для появления феномена фрагментированной политической реальности. Этот феномен подразумевает, что каждая группа или общество потребляет информацию в рамках заданных ценностных ориентиров и в рамках навязанной повестки. Феномен фрагментации создает возможности и сложности при проведении традиционной информационной работы в зарубежных государствах через социальные сети. Сегодня все государства столкнулись с необходимостью обращаться не ко всей аудитории национального государства, а к каждому отдельному сообществу, например к защитникам прав человека,

или патриотам, или противникам вакцинации и пр., причем с разными оценочными суждениями. Для понимания системы цифровых международных отношений необходимо знать следующий терминологический аппарат.

Киберпространство — это глобальная область взаимодействия, созданная набором вычислительных устройств, соединенных сетями, в которых хранится и используется электронная информация и происходит общение между участниками сети. До недавнего времени киберпространство считалось вопросом так называемой *low politics* — термин, используемый для обозначения незначительных или рутинных процессов в системе международных отношений. Напротив, «высокая политика» или *high politics* определяла традиционные вопросы мировой политики, которые имеют решающее значение для государства, его интересов и основополагающих ценностей и, как правило, являлись приоритетными на протяжении истории развития традиционной системы международных отношений, как, например, вопросы национальной безопасности, принятия внешней политических решений, дипломатии и т.п.

Традиционные международные отношения обозначают государство важнейшим актором, обладающим монополией на применение силы. Однако киберсфера и цифровые взаимодействия оказались новой движущей силой перераспределения власти и влияния в мировой политике, а также создания новых механизмов, с помощью которых различные акторы, отличные от государства, способны оказывать влияние на традиционные международные отношения.

Киберпространство формирует новые параметры международных отношений и новые измерения международной политики. Среди наиболее заметных нововведений — появление новых акторов — как официальных, так и неофициальных, — что меняет традиционный международный ландшафт принятия решений, создает новые угрозы и возможности для внешней политики и дипломатии. Например, пример работы неправительственной организации *WikiLeaks* демонстрирует политизацию и киберпространства, и возможности независимых акторов влиять на внешнеполитические институты государств.

Датафикация (datalization) — это бурный рост «цифровых следов» в интернете и массовое неконтролируемое использование аналитики больших данных в политических целях. Это формирует новые

особенности функционирования дипломатии и внешней политики, а именно: цифровую неопределенность, фрагментированную политическую реальность, а также противостояние так называемых фреймов. Самыми массовыми и понятными следами датафикации являются деятельность журналистов по расследованию коррупционных схем или информационные кампании, направленные на дискредитацию политических лидеров в социальных сетях, а также освещение журналистами таких кризисов, как сирийский или украинский. Еще одно следствие датафикации — это феномен политического цифрового вмешательства в избирательные кампании. Подобные акции основаны на аналитике данных, полученных из социальных сетей при помощи компьютерных программ или украденных при осуществлении кибератак. Отсутствие глобальных норм и договоренностей между акторами международной системы в использовании или рассекречивании цифровых следов создает новые повороты в деле использования информации в политических целях, включая напряжение отношений, отставки правительств и дестабилизацию социальной жизни. Такие события, как стратегия администраций социальных сетей по закрытию учетных записей (аккаунтов) отдельных политиков или российские инициативы о суверенизации интернета, также относятся к последствиям датафикации в международных отношениях, что необратимо и не может быть остановлено.

На традиционной дипломатической арене появляются новые вопросы, связанные с цифровым миром, и новые форматы взаимодействия, функционирующие в условиях крайней неопределенности и фрагментарности.

Цифровая неопределенность и фрагментированность подразумевают, что любой актор цифрового мира выступает в качестве политической силы, т.е. способен дестабилизировать ситуацию в стране и мире. Датафикация раздробила реальность на миллионы персонализированных кластеров или групп пользователей социальных сетей, которые оказывают влияние на восприятие мировой политики миллионами пассивных фолловеров. Жесткое информационное противостояние в цифровой среде, неприятие реальности, сконструированной другими группами, создает политическое напряжение, что может способствовать протестному движению в самых различных странах и, как следствие, выливаться в дипломатическое противостояние. При-

мером может служить разнообразие официальных трактовок событий протестных акций в Сирии в 2011 г., Белоруссии в 2021 г., в Вашингтоне в январе 2021 г. или Казахстане в январе 2022 г., представленных представителями МИД разных стран в социальных сетях, причем оценки событий относительно того, в какой из стран «бунт толпы», «терроризм» или «демократическая революция», зависели от национальных и политических целей. Это подразумевает, что любая новая появившаяся информация в социальных сетях способна изменить поведение политических элит или внешнеполитическую деятельность государства. Работа официальных каналов цифровой дипломатии может быть подорвана более эффективной информационной кампанией негосударственных акторов, включая блогеров, журналистов, кибердиссидентов и пр. Цифровизация раздробила международные отношения и информацию о происходящих событиях на миллионы конкурирующих трактовок, интерпретаций, причем в повествовательном и визуальном формате. Стейкхолдеры (владельцы) созданных политических реальностей и информации в интернете оказывают влияние на восприятие мировой политики миллионами пассивных фолловеров.

Фрагментированная цифровая реальность позволяет цифровой дипломатии формировать разные политические реальности в социальных сетях и сдерживать информационные кампании других государств или неправительственных акторов, продвигая собственную повестку, легитимируя собственные действия и делегитимируя действия противников. Примером может выступать работа различных виртуальных групп во время избирательной кампании в США в 2016 г. или цифровая тактика оппозиционных групп в Белоруссии или Судане в рамках мобилизации пользователей вокруг эмоциональных хэштегов. Наличие макро- и микрокластеров в социальных сетях может ограничивать и расширять действия и усилия государственной цифровой дипломатии. Некоторые государства и дипломаты воспользовались этой новой раздробленной реальностью для решения своих внешнеполитических задач.

Эффективность официальной цифровой дипломатии в эпоху датафикации зависит от понимания практиками такого понятия, как *фрейминг*, что подразумевает использование эмоций, тональности и различных практик для продвижения нужного нарратива или информации. Официальные каналы государств осуществляют так называемое фрей-

мирование событий в реальном времени для разных групп целевой аудитории, чтобы конкурировать с информацией, распространяемой СМИ, журналистами и другими акторами противоположной стороны. Понимание этого процесса создает новую основу для осуществления эффективной цифровой дипломатии. Наш анализ, который будет предложен ниже, полностью подтверждает, что умелое использование ключевых слов и тональности постов способствует продвижению массива месседжей через массу разрозненных пабликов, эхо-камер, пузырей фильтров, которые вместе и составляют фрагментированную цифровую реальность.

В итоге современные международные отношения — это уже не противостояние различных ценностей, политических систем экономик, а противостояние различных реальностей, которые из цифрового пространства попадают в традиционные каналы информационных потоков и оказывают влияние на политическую стабильность в различных странах.

Цифровая неопределенность и фрагментация требуют проведения наступательной цифровой внешней политики. Спонсируемые государством платформы международного вещания или цифровой дипломатии работают в условиях неожиданной и непредсказуемой конкуренции с блогерами, СМИ, которые в любой момент могут подорвать все усилия государственной информационной машины. Линейная дипломатия не работает, поскольку государственные каналы могут проигрывать информации, идущей от частных блогеров или СМИ. Хорошим примером выступает, например, ситуация в Венесуэле в 2019 г., когда каналы госдепартамента международного вещания США в сети Интернет, которые всегда были популярны в данной стране, потеряли свою привлекательность и аудиторию из-за резкого роста числа и популярности венесуэльских блогеров, СМИ и цифровой активности населения. Поэтому понятие киберсилы является основной концепцией для объяснения поведения официальной цифровой дипломатии государств, работающих в конкуренции с многочисленными каналами.

Киберсила — это способность дипломатии использовать киберпространство для создания преимуществ и влияния на события в других операционных средах. Она может быть как мягкой (основанной на привлечении и убеждении), так и острой (принуждающей, агрессивной). Основными инструментами выступают информационные и техно-

логические шаги — закрытие неудобных профайлов и источников нежелательной информации, создание информационных кампаний по дискредитации отдельных политических лидеров и государств, а также кибератаки, которые доводят до отказа интернет-систему компании или страны. Другие формы включают вставку вредоносного кода для взлома систем или кражи интеллектуальной собственности. Сюда же относятся специальные антицензурные программы, позволяющие преодолевать информационные барьеры и распространять информацию, а также деятельность хактивистов или идеологически мотивированных злоумышленников. В итоге действия мягких и жестких инструментов киберсилы произошло смыкание цифровой дипломатии с инструментами кибербезопасности и контроля за интернетом или его суверенными частями, что привело к появлению понятия кибердипломатии.

Кибердипломатия — это взаимодействие между государствами по чувствительным вопросам цифрового политического вмешательства, подрыва суверенитета государств, хакерских атак и выработки новых норм поведения в системе цифровых международных отношений. Новая система международных отношений в ее цифровом формате требует формирования нового пакета обязывающих документов для создания зон ответственности акторов, что сегодня медленно происходит на уровне двухсторонних отношений и работы постоянных рабочих групп в ООН.

Вопросы и аналитические задания

1. Дайте определение понятия «цифровые международные отношения» по монографии:
2. *Choucri N.* International Relations in the Cyber Age: The Co-Evolution Dilemma. Cambridge, Massachusetts: MIT Press, 2018.
3. Прочитайте следующую статью и дайте определения понятиям «цифровая неопределенность», «цифровая фрагментация» и «цифровая дипломатия»:
4. *Цветкова Н. А., Сытник А. Н., Гришанина Т. А.* Цифровая дипломатия и digital international relations: вызовы и новые возможности // Вестник Санкт-Петербургского университета. Международные отношения. 2022. № 2. С. 174–196.

5. Ознакомьтесь со следующим документом и дайте актуальное определение понятия *cyberdiplomacy*: *A Leaders' Guide to Building a Tech-Forward Foreign Policy, 2022* // Blair Institute for Global Change. <https://institute.global/policy/leaders-guide-building-tech-forward-foreign-policy#measure1>.
6. На основании анализа документа систематизируйте подходы дипломатии данных указанных государств: *Unheard Voice: Evaluating five years of Pro-Western Covert Influence Operations*. Report by Cyber Policy Center, Stanford University, 2022. <https://cyber.fsi.stanford.edu/publication/unheard-voice-evaluating-five-years-pro-western-covert-influence-operations-takedown>.

Рекомендованная литература

1. *Bjola C., Pamment J. Countering Online Propaganda and Extremism: The Dark Side of Digital Diplomacy*. N. Y.: Routledge, 2018.
2. *Choucri N. International Relations in the Cyber Age: The Co-Evolution Dilemma*. Cambridge, Massachusetts: MIT Press, 2018.
3. *Manor I. A Vocal and Volatile Online Public*, in *The Digitalization of Public Diplomacy*. Cham: Palgrave Macmillan, 2019.
4. *Tsvetkova N., Sytnik A., Grishanina T. Digital International Relations: Uncertainty, Fragmentation, and Political Framing* // *The Routledge Handbook of Russian International Relations Studies*. Lagutina M., Tsvetkova N., Sergunin A. (Eds.). N. Y., L.: Routledge, 2023. P. 381–395.
5. *Цветкова Н. А., Сытник А. Н., Гришанина Т. А. Цифровая дипломатия и digital international relations: вызовы и новые возможности* // *Вестник Санкт-Петербургского университета. Международные отношения*. 2022. № 2. С. 174–196.

Раздел 2

Кластеры в цифровых международных отношениях

Цифровые международные отношения включают следующие основные кластеры: информационная война, кибербезопасность и кибердипломатия, глобальное управление интернетом, цифровые избирательные технологии. Картирование кластеров системы цифровых международных отношений целесообразно обозначить в рамках категорий «противостояние» и «сотрудничество» по горизонтальной оси координат, а также ранжировать степень «прозрачности» и «секретности» в использовании цифровых инструментов по вертикальной оси координат. Происходит нарастание цифровых проблем, которые оказывают дестабилизирующее давление на традиционную систему международных отношений, включая проблемы политического вмешательства посредством хакерских атак, цифровой шпионаж, деятельность транснациональных групп кибердиссидентов и др. Но есть и группа вопросов, по которым проходит линия сотрудничества на уровне двухсторонних и многосторонних связей, а именно — глобальное управление интернетом. Более того, акторы используют скрытые и открытые цифровые инструменты для решения политических задач и вопросов национальной безопасности.

Картирование имеющихся кластеров показывает, что возможности сотрудничества открыты для таких вопросов, как глобальное управление интернетом или вопросы экономического характера. Сфера переговоров (кибердипломатия), которая занимается дипломатическим регулированием хакерских атак и их атрибуцией, также формирует возможности для соглашений между субъектами системы. Например, соглашение между США и Европейским союзом о нормах по регулированию трансатлантических потоков данных пространства в США и Европе, подписанное в марте 2022 г., а также исполнительный указ Дж. Байдена как следующий шаг реализации данного соглашения, подписанный в октябре 2022 г., выступают примером воз-

возможного сотрудничества [1]. Указанные кластеры находятся в постоянном движении, поскольку цифровые технологии почти ежедневно предоставляют новые инструменты для решения экономических, политических и военных задач. Но самое главное — объединяющим элементом для всех кластеров является цифровая дипломатия или дипломатия данных. Именно цифровая дипломатия выступает средством и сотрудничества, и противостояния между участниками киберсистемы, охватывая как открытые, так и скрытые действия государственных и негосударственных структур.

Сегодня мировая система находится в той точке развития новой киберсистемы, когда взаимодействие между странами, прокси-группами или пользователями в киберпространстве требует новых норм поведения государств и других акторов либо в духе Ялтинских/Потсдамских соглашений и проведения красных линий в интернете, либо в стиле пунктов В. Вильсона об открытой дипломатии. Большие данные и умелая аналитика цифровых следов оказывают влияние не только на пользователей социальных сетей, но и на традиционных акторов мировой политики — государства, — размывая их силу и влияние.

Другой точкой нестабильности выступает раскол интернета на зоны влияния или *киберсуверенитеты*. Борьба технологических суверенитетов и киберсуверенитетов, выраженная в стремлении распространить национальные границы на потоки данных и обособить часть интернета от влияния других акторов, лежит в основе концепции геополитической фрагментации, выдвинутой в рамках дискуссий по глобальному управлению интернетом. Действия государств или группы государств по зонированию киберпространства, ограничению нежелательной информации и ценностей приводят к формированию новой цифровой политики альянсов. Киберпространство становится местом непрерывной геополитической киберконкуренции. Вместе с этим происходит процесс навязывания норм управления сетью в соответствии с системой ценностей и внешнеполитических задач лидеров технологических процессов. Так, США предлагают подходить к вопросам фрагментации, связанным с регулированием трафика, с точки зрения прав человека, отстаивая правомерность демократических политических мер и делегитимируя отрицательную авторитарную фрагментацию как результат действий противников. Другим

примером выступает цифровая политика Китая в некоторых странах Азии или Африки, при которой государства делают выбор в пользу китайской модели регулирования цифрового информационного пространства, а не в пользу американской или российской модели. Сегодня стало ясно, что ни США, ни другие государства не могут противостоять концепции киберсуверенитета, как это было в 2010-е гг., а, наоборот, стараются использовать данную технологическую раздробленность в политических интересах.

Раздробление интернета на зоны влияния, рост влияния негосударственных акторов привели к появлению фрагментированной политической реальности. Наличие сотни мнений о событиях международной жизни формирует новые условия принятия решений под влиянием цифровой политической активности различных заинтересованных групп. В 2022 г. США заявили о том, что цифровые данные являются источником геополитической власти или цифровой силы. Следовательно, необходимо консолидировать коалицию союзников вокруг единых норм поведения в интернете и в то же время усиливать дипломатическое и экономическое давление на противников, включая кибероперации и санкции в отношении конкретных стран. Этот подход стал стратегией новой так называемой внешней киберполитики США, которая была обозначена осенью 2022 г. [2]. В итоге феномен фрагментации интернет-пространства создает сложности и возможности при проведении традиционной информационной работы в зарубежных государствах.

В настоящий момент существует порядка 80 государств, которые активно используют цифровую силу в своей внешней политике.

Цифровая сила, определяемая нами как возможности для государства приводить в движение общество, влиять на политические шаги других стран при помощи цифровых технологий, меняет традиционный расклад влияния государств на карте мировой политики. На лидирующие позиции выходят Китай, Египет, Индия, Иран, Ирак, Израиль, Мьянма, Пакистан, Филиппины, Россия, Саудовская Аравия, Украина, ОАЭ, Великобритания, США, Венесуэла, Вьетнам и ряд других государств. Многие из них, казалось бы, не претендуют на первенство в глобальной политике. Но в киберпространстве именно эти государства создали масштабный аппарат цифровой дипломатии, осуществляют глобальные или региональные информационные

кампании, а также внедрили ряд технологических приемов, включая пропаганду, хакерские атаки, шпионаж и многое другое, что еще несколько лет назад осуждалось дипломатами и внешнеполитическими экспертами. Эти страны, обладающие цифровой силой, передают свой опыт в области контроля за киберпространством или сдерживания кибератак другим странам, образуя новые линии сотрудничества в киберсистеме. Например, Китай, продолжая настаивать на том, что продвигаемые США принципы не могут претендовать на моральную универсальность, продвигает свои технологические наработки, ценности и нормы взаимодействия с сетевыми ресурсами в тридцать других государств. Трансфер китайских подходов формирует законодательство и политические стратегии стран о кибербезопасности или об управлении социальными сетями. Египет, Лаос, Пакистан, Уганда, Вьетнам, Зимбабве и многие другие государства приняли законы в данной области, которые отражают китайские правила.

Важным вопросом, который стоит на повестке вектора развития цифровой системы международных отношений, является появление новых альянсов или, наоборот, усиление односторонней цифровой политики традиционных государств. Как будут действовать США, Россия, КНР и другие страны, которые стали обладателями цифровой мощи в новой системе? Будут ли они выстраивать альянсы на основе имеющихся традиционных ценностных и стратегических ориентиров, или киберпространство ликвидирует традиционные полюса силы и создаст новые, исходя из приобретенных технологических мощностей и возможностей влияния? Современная политика в цифровом пространстве различных государств свидетельствует о том, что формируется так называемая сетевая политика, при которой многие государства, не подходящие под систему ценностей условного лидера, становятся частью сети экономического и политического влияния. Формирование группы государств, которые стремятся следовать за технологиями и придерживаться норм поведения и контроля в интернет-пространстве, происходит в части цифровой дипломатии США, КНР и других государств.

Со стороны США, Россия, Китай и Иран обозначены как основные территории для применения дипломатии данных США, что показывает контуры цифрового противостояния. На российском направлении предусматривается сдерживание реализации глобальных проектов

России в цифровой сфере на Ближнем Востоке, в Европе и Латинской Америке, а также в Центральной Азии посредством взаимодействия с местной цифровой средой, а также посредством развития активной цифровой дипломатии и международного вещания США в странах этих регионов. На китайском направлении предпринимаются меры по противодействию международному вещанию посредством создания эффективных контрнарративов. На иранском направлении ведется активное препятствование распространению пропаганды правительства Ирана как внутри страны, так и за ее пределами. В свою очередь, Россия и Китай подписали соглашение «О сотрудничестве в области обеспечения международной информационной безопасности», а США и Европейский союз договорились об обмене данными пользователей и о создании единого киберпространства в рамках трансатлантических ценностей. Сюда же относится инициатива США о подписании Декларации будущего интернета [3]. Более 60 стран согласились поддерживать либеральные нормы и противодействовать китайской и российской моделям контроля интернета. При этом в интернет-сообществе, в том числе и в США, слышны голоса критики в отношении Декларации. Несмотря на обозначенную приверженность принципам прав человека, документ рассматривается как еще один шаг на пути к конфронтации и созданию киберпространства только «для своих», тем самым увеличивая его фрагментированность. Все подобные действия отражают процесс бурления внутри цифровых международных отношений, показывают попытки традиционных акторов удержать нити власти в Сети среди миллионов пользователей, организаций и сообществ — новых акторов системы международных отношений.

Примечания

- [1] European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework // European Commission, March 25, 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087.
- [2] National Security Strategy 2022 // The White House. <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>.

[3] Declaration for the Future of the Internet, The Department of State, April 28, 2022. <https://www.state.gov/declaration-for-the-future-of-the-internet>.

Вопросы и аналитические задания

1. На основании анализа документа сделайте оценку цифровой мощи ведущих государств: *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*. Oxford 2021. demtech.oii.ox.ac.uk.
2. На основании анализа документа систематизируйте рекомендации экспертного сообщества для выработки цифровой политики: *Fick N. Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet* // Council on Foreign Relations. Independent Task Force Report. No. 80. 2022.
3. Что такое киберсуверенитет?
4. Как государства используют свою цифровую мощь?

Рекомендуемая литература

1. *Hocking B., Mellisen J. Diplomacy in the Digital Age*. Clingendael Report. Netherlands Institute of International Relations Clingendael, 2015.
2. *Manor I. The Digitalization of Public Diplomacy*. Palgrave Macmillan, 2021.
3. *Manor I., Bjola C. Public Diplomacy in the Age of 'Post-Reality'* // *Public Diplomacy and the Politics of Uncertainty*. Surowiec P., Manor I. (Eds.). L.: Palgrave Macmillan, 2019. P. 111–143.
4. *Tsvetkova N., Sytnik A., Grishanina T. Digital International Relations: Uncertainty, Fragmentation, and Political Framing* // *The Routledge Handbook of Russian International Relations Studies*. Lagutina M., Tsvetkova N., Sergunin A. (Eds.). N.Y., L.: Routledge, 2023. P. 381–395.
5. *Цветкова Н. А., Сытник А. Н., Гришанина Т. А. Цифровая дипломатия и digital international relations: вызовы и новые возможности* // *Вестник Санкт-Петербургского университета. Международные отношения*. 2022. № 2. С. 174–196.

Раздел 3

Механизм и особенности развития цифровых международных отношений

Новые тренды в период цифрового раскола: кибердипломатия

В складывающейся системе цифровых международных отношений дипломатия выступает единственной формой поиска стабилизации и реакции на вызовы и противостояния в информационной среде или в социальных сетях. Чтобы реагировать на указанные вызовы, государства стремятся институционализировать цифровую дипломатию, создавая новые отделы в области аналитики данных, кибербезопасности, а также формируют различные группы переговорщиков по проблемам управления интернетом, например на базе ООН.

Технологии стали частью дипломатии и дипломатического торга, что привело государства к мысли о необходимости создания отдельного аппарата по *кибердипломатии* — института транслирования технических угроз на политический и дипломатический языки и последующего использования цифровых возможностей во внешней политике. США, страны Европы, Бразилия, Австралия и некоторые другие государства создали институт кибердипломатов (*cyber ambassadors*), в задачи которых входят анализ цифровой политики страны аккредитации, взаимодействие со специалистами в области IT-технологий и формирование реакции на вызовы в социальных сетях или в сфере информационной безопасности.

Например, в США таким опорным пунктом в кластере «сотрудничество» является Отдел по киберпространству и цифровой политике (Bureau of Cyberspace and Digital Policy), созданный администрацией Дж. Байдена в 2022 г. Подразделение по международной информационной и коммуникационной политике осуществляет поддержку инноваций и цифровой экономики, мультистейкхолдерного подхода к глобальному управлению интернетом в соответствии с ценностями и внешнеполитическими приоритетами США, а подразделение по обе-

спечению доступа к интернету занимается вопросами модерирования контента, взаимодействия с цифровыми платформами и способствует продвижению цифрового активизма. В кластере «противостояние» действует отдел по внедрению новых технологий (*Technology Engagement Team*), сформированный в рамках Центра глобальной информации (*Global Engagement Center*). Взаимодействуя со Службой по искусственному интеллекту и перспективным технологиям (*Artificial Intelligence and Emerging Technology Office*) и с 2019 г. с технологическими гигантами Кремниевой долины, отдел реализует программы мониторинга данных в социальных сетях для противодействия иностранной дезинформации и пропаганде, разрабатывает методы борьбы с нарративами, которые не соответствуют интересам и ценностям США, способствует тестированию и внедрению в процессы обработки информационных потоков инструментов на основе новых технологий, больших данных и искусственного интеллекта.

Цифровая дипломатия обладает разными по качеству инструментами, и нельзя сказать, что все страны находятся на одном уровне понимания в использовании технологических разработок. Более того, инструменты, которые для каких-то государств стали уже забытым прошлым, могут выступать эффективным средством в дипломатическом арсенале многих стран. Кто-то из дипломатов остановился на уровне использования линейной цифровой дипломатии с прямым диалогом и без политизации, а какие-то страны активно привлекают сторонние организации или частных лиц для осуществления киберопераций. Но чаще всего лидирующие государства используют все имеющиеся инструменты, и можно сказать, что в цифровой дипломатии нет устаревших методов или подходов.

Если цифровая дипломатия 2010-х гг. являлась частью публичной дипломатии, субъектом цифровизации, а дипломаты посредством линейного распространения информации в социальных сетях пытались оказывать влияние на всю зарубежную аудиторию, информируя о событиях, то дипломатия данных 2020-х гг. — это использование алгоритмов фильтрации аудитории, контента и цифровых социальных взаимодействий, построение информационных кампаний и поиск источников недружественной информации. В период 2015–2017 гг., когда появилось огромное число акторов в социальных сетях и инструментов для продвижения информации, цифровая дипломатия

стала базироваться на фундаменте создания сетей влиятельных лиц (инфлюэнсеров), которые обладают авторитетом у своих подписчиков, что представлялось более эффективным инструментом для продвижения позиции государства и борьбы с конкурентами, чем линейное распространение информации. Во внешнюю политику пришла идея об алгоритмах для транслирования пользователям таргетированной информации. Стали появляться проекты по нейтрализации пропаганды экстремистов и проекты по влиянию на малые социальные группы в интернете.

Однако и этот этап в развитии цифровой дипломатии был смещен в 2018–2022 гг., когда произошел неконтролируемый доступ самых разных акторов к технологиям искусственного интеллекта. В финальном отчете о почти двухлетней работе американской Комиссии национальной безопасности в области искусственного интеллекта (National Security Commission on Artificial Intelligence) обозначен переход к геополитическому соперничеству в области перспективных технологий, что также нашло отражение в Стратегии национальной безопасности 2022 г. Искусственный интеллект и другие технологии будущего реорганизуют мировой порядок, повлияют на характер сотрудничества и конфликта. При этом, согласно документу, США должны занять лидирующую позицию, чтобы сформировать коалиции и режимы преференций. В достижении этих целей значительная роль отводится усилиям американской дипломатии.

США заявляют о приверженности подходу двойного взаимодействия (*dual-track approach*). Он предполагает, с одной стороны, отход от стратегической конкуренции в тех областях, которые представляют взаимный интерес как для США, так и для их соперников, с другой — более тесное сотрудничество с демократическими режимами. Однако возможности, предоставляемые перспективными цифровыми технологиями, такие как гиперперсонализация контента, аналитика социальных и психологических профилей на основе цифровых взаимодействий, поисковых запросов, электронных покупок и других цифровых следов, которые имеются у брокеров данных и доступны IT-гигантам, активно применяются и негосударственными акторами, что связано со слабым регулированием данной сферы. Это позволяет зачастую обычным пользователям стать агентами влияния на цифровую аудиторию при помощи создания эффективных информационных

кампаний, механизмов фильтрации контента, синтетических СМИ и дипфейков. Цифровым дипломатам стало ясно, что без применения аналитики больших данных уже невозможно выстроить цифровую информационную кампанию или оказать влияние на целевые аудитории, а без сотрудничества в области международной информационной безопасности, а также без выработки норм и правил ответственности в цифровом пространстве невозможно выстраивать долгосрочные отношения как в физической, так и в цифровой реальности.

Цифровая дипломатия государств

Именно неопределенность в поведении акторов в области применения цифровых технологий и фрагментация киберпространства требуют проведения наступательной цифровой дипломатии. Спонсируемые государством платформы международного вещания или цифровой дипломатии работают в условиях конкуренции с блогерами, СМИ, которые в любой момент могут подорвать все усилия государственной информационной машины. Государственные каналы могут проигрывать информации, идущей от рядовых пользователей. Хорошим примером выступает, например, ситуация в Венесуэле в 2019 г., когда каналы международного вещания США в сети Интернет, которые всегда были популярны в данной стране, потеряли привлекательность и аудиторию из-за резкого роста количества и популярности венесуэльских блогеров, СМИ и цифровой активности населения, что оказало влияние на удержание власти действующим президентом. Правительственные и неправительственные акторы стали важнейшими игроками в цифровом противостоянии.

Цифровая дипломатия может выступать в качестве одного из инструментов «управления неопределенностью» благодаря своевременному выявлению угроз и противодействию им. В рамках кластера «противостояние» действия будут охватывать как распространение, так и своевременное предупреждение нарративов, фреймов и образов, направленных на продвижение интересов отдельных государств и частных компаний. Новые модели восприятия и регулирования распространения информации упрощают влияние на поведение пользователей за счет использования дипломатии алгоритмов в социальных сетях, позволяя достигать внешнеполитических целей эффективными и менее затратными способами. Но чаще всего цифровая дипломатия включа-

ет в себя стратегию *гейткипинга*, когда закрывается доступ тем акторам, кто подвергает опасности интересы основных держателей каналов.

Вовлеченность в интернет-пространство самых разных слоев населения делает невозможной реализацию цифровой внешней политики только при помощи правительственных ведомств. На новом этапе развития механизм цифровой дипломатии и кибербезопасности задействован в создании рамок для построения сотрудничества и ведения конфликтов в цифровом пространстве. В то же время он включает в себя неофициальную армию поддержки в лице IT-компаний, частных пользователей (от цифровых активистов до знаменитостей), независимых организаций, а также дюжину исследовательских центров в университетах и активных политиков, которые могут выступать единым и значимым звеном в реализации внешней политики. Кризис на Украине демонстрирует пример использования многообразия акторов в цифровой внешней политике США при объединении содержания информации. В социальных сетях обнаруживается не только активная деятельность и единство постов государственного аппарата цифровой дипломатии США, но впервые проявилась цифровая вовлеченность около 900 американских политиков, которые продвигали тезисы информационной кампании в поддержку позиции Киева. Несомненно, сам кризис вызывал активизацию политического истеблишмента США, но показательно проявилось единство политической позиции среди американских участников групп. Конгрессмены, политики, дипломаты и частные блогеры поддерживали и цитировали основные смысловые посты правительственных каналов. Это способствовало тому, что малопопулярные каналы государственной цифровой дипломатии и международного вещания США попадали в топ-250 аккаунтов из миллионов каналов, где обсуждалась тема кризиса.

Украинский кризис привнес несколько новых трендов в цифровую дипломатию. Произошли изменения в содержании месседжа самых различных акторов, в основном американских, российских и европейских, но есть и примеры китайских. Цифровые ресурсы стали использоваться для информационного устрашения противников, что крайне редко наблюдалось ранее. Например, январская волна информационной кампании 2022 г., направленная на пропаганду последствий для России возможной операции, в марте — июне 2022 г. сменилась волной дискредитации политиков и ценностей России. Третья волна информа-

ционной кампании сконцентрировалась на сарказме и дискредитации посредством распространения визуальных образов. Для обозначения политики, когда государства используют юмор для фрейминга событий в целях продвижения национальных интересов, деконструкции критики со стороны оппонентов и противоборствующих нарративов, была предложена концепция стратегического юмора в публичной дипломатии. Все эти волны отражались в едином содержании месседжа, продвигаемого политическими фигурами, дипломатами, международным вещанием и цифровой дипломатией, исходящего от государственных каналов США и Европы. Более 3 млн. твитов на английском, русском и украинском языках на платформе Twitter,^{*} которые содержали #Украина на разных языках с конца 2021 г. по конец 2022 г., показывают эти изменения в методах цифровой дипломатии США.**

Более того, к 2022 г. сработал эффект традиционной публичной дипломатии, которая была направлена на создание сети блогеров, поддерживающих или цитирующих повестку каналов США или Украины. Киберармия независимых экспертов, исследователей и активных пользователей выступает основным звеном в создании так называемой дипломатии мемов, сарказма и юмора. Ранее подобный подход редко использовался правительством США в других странах. Визуализация контента, устрашение и дискредитация противника, а также исполь-

* Социальная сеть заблокирована в РФ. Доступ к сайту ограничен на основании статьи 15.3 федерального закона «Об информации, информационных технологиях и о защите информации».

** Выбор именно этого хэштега был обусловлен неформальным правилом использования хэштега страны для донесения информации до целевой аудитории, и во всех твитах содержалась информация или обсуждение проблемы по Украине. С помощью языка программирования Python и запроса «SQL» в базу данных PostgreSQL была осуществлена классификация наиболее популярных твитов и самых влиятельных аккаунтов, что позволило определить место акторов аккаунтов разных стран, включая США, среди лидеров общественного мнения в глобальной дискуссии по событиям на Украине. Мы классифицировали популярность местных блогеров, различных радикальных организаций и пр. Были выбраны 250 самых влиятельных каналов за каждый месяц. Влиятельность постов, или их информационный охват, измеряется путем подсчета числа информации пользователями или репостов, комментариев и построения маршрута репостов пользователей и их уровней. Другими словами, в современной цифровой дипломатии влиятельность — это масштаб взаимодействия команды дипломатов или индивидуальных блогеров с аудиторией, исчисляемый, как правило, количеством репостов.

зование сарказма оказались фронтлайнерами цифровой дипломатии. Законы о санкциях против России предоставляли финансирование для таких проектов, которые сдерживают распространение российской информации в странах Европы и США. В знаменитом законе о санкциях от 2017 г. (*Countering America's Adversaries Through Sanctions Act*) международное вещание, мониторинг социальных сетей, взаимодействие с ключевыми блогерами и журналистами в Европе и Евразии были обозначены в качестве основных инструментов сдерживания России в Европе. Конгресс США выделял ежегодное финансирование в размере от 250 млн. долл. в 2017 г. до 295 млн. долл. в 2022 г. для проекта под названием *Countering Russian Influence Fund*. Эти деньги предназначены для стран НАТО в рамках реагирования на информационные вызовы со стороны России.

Соединение правительственных каналов с многочисленными креативными организациями на Украине способствовало тому, что международное вещание США стало востребовано целевой аудиторией не только на Украине, но и в других странах, теми пользователями, кто интересовался вопросами кризиса. Как правило, каналы международного вещания США не занимают лидирующих мест среди аудитории в зарубежных странах. Благодаря программам обучения и формирования института суррогатов эти каналы оказываются основным хабом, где циркулирует информация, предназначенная для дальнейшего цитирования и распространения по сайтам дружественных журналистов и СМИ. Около 15 каналов правительственной цифровой дипломатии не покидали лидирующих позиций среди 250 влиятельных каналов на платформе Twitter^{***} по теме Украины. Их информация постоянно цитировалась и использовалась американскими политиками и дипломатами, которые активно включились в информационное противостояние с Россией.

Большинство популярных постов на платформе Twitter,^{****} как со стороны США, так и со стороны Украины и других стран, публи-

^{***} Социальная сеть заблокирована в РФ. Доступ к сайту ограничен на основании статьи 15.3 федерального закона «Об информации, информационных технологиях и о защите информации».

^{****} Социальная сеть заблокирована в РФ. Доступ к сайту ограничен на основании статьи 15.3 федерального закона «Об информации, информационных технологиях и о защите информации».

куются на английском языке, что свидетельствует о выстраивании линии взаимопонимания и сотрудничества между пользователями, которые готовы поддержать позицию США и информационную кампанию на английском языке. Еще в ноябре 2021 г. английский язык не доминировал по вопросам Украины. Резкий рост числа публикаций появился в конце декабря 2021 г. — начале января 2022 г., захватывая только тех пользователей, которые продвигают трансатлантическое партнерство между США и Украиной или между Европой и Украиной и которые готовы апеллировать к западной аудитории и обсуждать кризис на английском языке. Несомненно, сыграла свою роль политика ограничения работы платформы в России, но формирование нарратива для массы европейцев, украинцев, американцев на английском языке имеет важнейшее значение. Как это ни парадоксально, один из продвигаемых принципов языкового разнообразия в киберпространстве становится новым источником фрагментации, а линия возможных договоренностей, лоббизм и давление проходят в области языковой политики и устанавливаются антироссийским содержанием постов. Данный пример цифровой внешней политики создает известный эффект информационного пузыря, в котором формируется виртуальная политическая реальность, весьма далекая от реальных событий. Однако любой отдельный пост в условиях такой фрагментации оказывает влияние на принятие политических решений, обозначая зарождающиеся альянсы и противостояния.

Еще одним примером выступает цифровая дипломатия США в регионе Центральной Азии. Государства региона следуют различным подходам к регулированию киберпространства. В каких-то странах разрешены все социальные сети, где-то платформы заблокированы. Подобные технологические разрывы используются правительством США. После изменения международной обстановки и формирования новой внешней политики России США стали активно вовлекать целевые аудитории данного региона в свою повестку. США стремятся убедить аудиторию государств Центральной Азии в необходимости отказа от сотрудничества с Россией. Сегодня созданы порядка 15 специальных профилей на различных платформах. Информационная кампания проходит на русском языке. Несколько месяцев посты не получали популярности среди целевой аудитории. Эффективность данной информационной кампании стала набирать обороты, когда США перешли

к использованию поддельных учетных записей и СМИ. Для изменения лиц и фамилий известных персонажей стандартно применяется технология дипфейков. Особую эффективность показали фиктивные СМИ: они выдавали себя за независимые новостные агентства, освещающие события в Центральной Азии. Примерами выступают «Восточная правда» и «Фактограф». СМИ декларировали, что основное внимание уделяется развенчанию мифов и распространению фактов о Центральной Азии. Публикуя местные новости, СМИ призывали аудиторию к саботажу против России. Более того, такие синтетические средства массовой информации аккумулировали тексты американских каналов международного вещания и стоковый ресурс *central.asia-news.com*, известный в региональной цифровой дипломатии США.^{*} После начала специальной военной операции на Украине США стали активнее использовать *Telegram* для влияния на целевую аудиторию. Однако отметим, что наблюдается некоторое недоверие к данной платформе. Оно выражается в отказе от верификации каналов, работе в ограниченном сегменте целевой аудитории, создании каналов-ботов и каналов-ретрансляторов. Нами были проанализированы 45 каналов цифровой дипломатии США на 19 языках на платформе *Telegram*. Поскольку США не могут напрямую осуществлять контроль данного сегмента социальных сетей, активность каналов не так высока, как на платформах, принадлежащих американским IT-гигантам. Созданные начиная с 2015 г. каналы публикуют контент на английском, русском и государственных языках и направлены на вовлечение аудитории из России, стран постсоветского пространства, Ирана. Наш анализ показывает, что приоритетными странами являются Кыргызстан, Узбекистан, Таджикистан и Иран. В основном работа ведется в небольших группах участников или выпускников программ публичной дипломатии США (*FLEX*, *TechCamp*). Другой характерной чертой является персонализированный характер вовлечения, то есть часто контент создается наиболее активными подписчиками каналов. Интерес также представляет стремление охватить аудиторию не только

^{*} *central.asia-news.com* (Caravanserai / Каравансарай) — сайт на русском и узбекском языках, спонсируемый Объединенным центральным командованием ВС США, созданный с целью «развития региона в сторону обеспечения большей региональной стабильности на основе двусторонних и многосторонних договоренностей».

на государственном языке страны, на которую вещает канал, но и на национальных языках отдельных народов, входящих в ее состав (например, на татарском в России и на оромо в Эфиопии). Такой подход может быть обусловлен как принципом мультикультурализма, так и стремлением использовать фрагментацию по языковым и культурным линиям в политических целях. Однако не самые высокие медиапоказатели, например, для канала на татарском языке могут свидетельствовать о неэффективности этого подхода.

Такой поворот в сторону Центральной Азии не наблюдался ранее в цифровой дипломатии США. Сегодня уже не имеет смысла заниматься поиском и развенчанием подобных информационных кампаний. Они стали частью цифровых международных отношений и моральным выбором того или иного государства. Когда-то правительство США обвиняло Российскую Федерацию в использовании злонамеренных цифровых инструментов во время президентской избирательной гонки 2016 г. Раскрученная кампания против России (*Rusgate*) выявила различные подходы, которые могут быть использованы в цифровой внешней политике. США, обвиняя российское правительство в неприглядных методах цифрового давления, активно используют их во внешней политике. Отсутствие норм и договоренностей в сфере распространения информации позволяет всем странам, без оглядки на провозглашаемые ценности, использовать различные методы для дискредитации политики других государств.

Цифровая дипломатия оказалась на пересечении линий сотрудничества и конфронтации в цифровых международных отношениях. Она выступает основным инструментом применения цифровой силы государств и других акторов. Она также выступает основным звеном для ведения переговоров по вопросам кибербезопасности или информационных кампаний. Цифровая дипломатия всё еще проходит этап институционализации в дипломатической системе всех стран, обрстая методами, экспертами и отделами в МИД. Формирующиеся механизмы цифровой дипломатии позволяют политикам и цифровым дипломатам использовать фрагментацию киберпространства в условиях геополитического соперничества для достижения внешнеполитических целей. Бурное развитие новых технологий и методов сбора и управления данными, которые становятся стратегическими ресурсами, определяющими технологическую мощь государств в цифровых

международных отношениях, приводят к появлению зон турбулентности и точек бифуркации, что способно привести систему в нестабильное состояние. Иногда оно характеризуется как состояние глобальной неопределенности, когда фрагментированность киберпространства и стремление каждого государства обеспечить свой киберсуверенитет лишает ряд акторов глобального влияния и позволяет контролировать только фрагмент сети. С помощью цифровых методов, подкрепленных большими данными и искусственным интеллектом, в образовавшихся фрагментах формируются различные политические реальности, что усиливает неопределенность. При этом агентами, определяющими поведение и решения более влиятельных акторов, становятся обычные пользователи. Складывающаяся система требует стабилизации за счет участия как государственных, так и негосударственных акторов в выработке рамок и подходов к ведению противостояний и установлению сотрудничества в киберпространстве.

Цифровая дипломатия международных организаций и альянсов: ООН и НАТО

Цифровая дипломатия международных организаций, в отличие от работы национальных дипломатов или МИД, ориентирована на многозадачность, что размывает стратегию и создает препятствия на пути мобилизации целевой аудитории. Мы продемонстрируем два существующих подхода в цифровой дипломатии международных организаций: линейная цифровая дипломатия ООН и цифровая дипломатия алгоритмов НАТО. В ООН за цифровую активность отвечают Департамент глобальных коммуникаций (*UN Department of Global Communication*) и особая команда по работе в социальных сетях (*Social Media Team*). Департамент имеет три подразделения: стратегических коммуникаций (*Strategic Communication Division*), новостей и медиа (*News and Media Division*), внешних контактов (*Outreach Division*). Платформа Twitter* остается наиболее подходящей для донесения информации и позиции ООН и Генерального секретаря. Контент публикуется

* Социальная сеть заблокирована в РФ. Доступ к сайту ограничен на основании статьи 15.3 федерального закона «Об информации, информационных технологиях и о защите информации».

на шести официальных языках. Помимо персональных аккаунтов глав департаментов и аккаунтов организаций, входящих в структуру ООН (UNICEF, UNESCO и UNHCR), наиболее важные новости аккумулируются на странице *UN News*.

Несмотря на довольно широкий охват аудитории, ее *вовлеченность* (среднее количество комментариев, ретвитов и лайков по сравнению с общим количеством подписчиков) на данных каналах остается довольно низкой. Два фактора снижают эффективность информационных кампаний ООН и удержание аудитории в диалоге: размытость повестки и многообразие источников сообщений. Например, в период 2020–2022 гг. самое большое количество постов относилось к борьбе с пандемией (хэштеги *#COVID19*, *#OnlyTogether*) и с изменением климата (хэштеги *#ClimateAction*, *#DecadeOfAction*, *#GreenCitizens*). ООН публиковала привлекательные визуальные образы, качественные снимки и инфографику, а аккаунты придерживались единого стиля оформления. Тем не менее указанная повестка не вызвала должного отклика аудитории. Комментарии носили критический характер и касались бездействия ООН по ряду вопросов. Чаще всего пользователями продвигались контрнарративы геноцида (хэштег *#TigrayGenocide*), эскалации конфликтов (хэштег *#Yemen*), что указывалось под постами ООН. Отсутствие ответов на комментарии обеспечило слабое вовлечение в диалог с аудиторией и оказывало влияние на реальную поддержку проектов ООН.

Цифровая дипломатия линейна, т.е. направлена на прямое распространение сообщения в монологическом формате, что сегодня малоэффективно в цифровой дипломатии.

Пример цифровой дипломатии НАТО показывает более активный подход к распространению информации. Это подход основан на следующем: 1) анализе больших данных; 2) оценке предпочтений аудитории и 3) тактике информационной войны при помощи устрашения.

НАТО как военно-политический блок, объединяющий 30 стран-членов, накопил большой опыт в работе с аудиторией и распространением информации за годы существования и противостояния с СССР и Россией. Данная деятельность осуществляется Службой информации НАТО (*NATO Information Service*). В 1999 г. был создан Центр медиа-операций НАТО (*NATO Media Operations Centre*), в 2003 г. — Отдел публичной дипломатии НАТО (*NATO Public Diplomacy Division*),

а также серия информационных центров в Европе, которые отвечают за противостояние с российской информацией в социальных сетях. Альянс постоянно наращивает присутствие в новых медиа. Все высшие должностные лица имеют аккаунты в социальных сетях. Цифровая дипломатия альянса подчиняется таким задачам, как: внутреннее сплочение организации, продвижение положительного образа организации на международной арене, противодействие угрозам и выстраивание коммуникации с оппонентами.

В социальных сетях НАТО продвигает *силовой военный нарратив*, публикуя соответствующие визуальные образы (оружие, военная техника, карты присутствия контингента в Европе). При создании и продвижении повестки использованы «силовые» хэштеги: #StrongerTogether, #WeAreNATO с публикацией соответствующих эмодзи (флагов стран, иконических символов силы), а также лексические единицы, относящиеся к понятию «сила»: *strong, strength; unity, allies, alliance, cooperation, support*. Используя маркетинговые приемы, НАТО конструирует образ «защитника Европы» с помощью высокочастотных для данной повестки единиц: *defense, defensive, protect and defend, defend democracy, Euro-Atlantic / European security, proportionate, response*. Тональность данных сообщений неизменно мажорная и позитивная. Кроме того, НАТО формирует образ «России-агрессора» за счет клишированных фраз с негативной оценкой: «*Russian aggression*», «*Russia's aggressive actions*», «*Russia's military build-up*».

Таким образом, НАТО в полной мере применяет информационную силу не только с целью поддержания собственной легитимности для стран-членов, но прежде всего для дискредитации и устрашения оппонента. Цифровая активность НАТО носит не только конструирующий и легитимационный характер, но определяется как информационные операции, и ее необходимо рассматривать в контексте информационных войн.

В итоге цифровая дипломатия, обладая высокой степенью персонализации, призвана осуществлять несколько целей:

- формировать цифровую идентичность за счет распространения нарратива о миссии и целях государства или организации. Социальные медиа выступают в качестве пространства диалога с глобальной аудиторией и «усилителем» воздействия нарратива, формируемого на основе ценностей, зафиксированных в документах;

- поддерживать репутацию, которая в большинстве случаев понимается как социально-когнитивный феномен, содержащий символический компонент и характеризующий способность группы или организации идентифицировать себя положительным образом для внешних акторов;
- поддерживать собственную легитимность в глазах глобальной общественности — одна из ключевых отличительных черт цифровой дипломатии международных организаций. Создание легитимности для входящих в состав организации государств и для своей аудитории позволяет укреплять существующие партнерские отношения, привлекать новых членов и финансирование;
- получать представление о мнениях и восприятиях глобальной аудитории для дальнейшего формирования повестки, включая «обоснование институциональных реформ, фрейминг реализуемой политики, использование ценностных символов и других риторических средств»;
- использовать социальные медиа для осуществления нормативной силы. Базовой предпосылкой данного подхода (*outside-in approach*) является создание ценности для аудитории с учетом ее мнений и предпочтений;
- выстраивать отношения с оппонентами — данная цель касается скорее деятельности, связанной с распространением стратегических нарративов и контрнарративов, которые рассматриваются в контексте информационных и гибридных войн.

Вопросы и аналитические задания

1. Охарактеризуйте новые подходы цифровой дипломатии государств на примере США.
2. Какие возможности предоставляет дипломатам цифровая неопределенность и фрагментация?
3. Осуществите анализ линейной цифровой дипломатии МИД и посольств:
 - Выберите МИД любой страны и 1–2 посольства из разных регионов.
 - Существуют ли отделы по *digital diplomacy*, *cyber diplomacy* или, наконец, *public diplomacy* в данном МИД? Если МИД создал

специальные ведомства для цифровой дипломатии/дипломатии данных, то каковы их функции? Есть ли открытый доступ к отчетам подразделений МИД по цифровой дипломатии?

- Проанализируйте профайлы МИД или посты министра, его пресс-секретарей в доступных социальных сетях относительно содержания формальных месседжей. О чем повествуют посты?
 - Найдите профайлы посольства выбранной страны в стране аккредитации и проанализируйте содержание постов, а также цифровую активность посольства: взаимодействует ли МИД с целевой аудиторией через социальные сети? Ведет ли посол свой личный блог для налаживания диалога с местной общественностью? Есть ли ответы МИД или посольств на комментарии под постами? Существует ли хэштеговая дипломатия?
4. *На основании анализа документа сделайте оценку цифровой мощи ведущих государств: Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. Oxford 2021. demtech.oii.ox.ac.uk.*

Рекомендуемая литература

1. *Лебедева М. М., Зиновьева Е. С.* Технология международных переговоров в цифровую эпоху. М.: Аспект-пресс, 2022.
2. *Сучков М. А.* «Геополитика технологий»: международные отношения в эпоху Четвертой промышленной революции // Вестник Санкт-Петербургского университета. Международные отношения. 2022. № 2. С. 138–157.
3. *Bjola C., Zaiotti R.* Digital Diplomacy and International Organizations. Autonomy, Legitimacy and Contestation. L.: Routledge, 2021.
4. *Manor I.* The Digitalization of Public Diplomacy. Palgrave Macmillan, 2021.
5. *Olsson E.-K., Wagnsson Ch., Hammargerd K.* The Use of Political Communication by International Organizations: The Case of EU and NATO Countering Online Propaganda and Extremism // The Dark Side of Digital Diplomacy. Bjola C., Pamment J. (Eds.). L.: Routledge, 2019. P. 66–80.

Раздел 4

Методы анализа цифровых международных отношений

В складывающейся системе цифровых международных отношений дипломатия выступает формой поиска стабилизации и реакции на вызовы и противостояния в социальных сетях. Цифровая дипломатия или дипломатия данных является самым быстрорастущим аппаратом в системе внешней политики всех стран и поэтому является основным предметом для научного анализа. В данном разделе будут представлены актуальные научные методы изучения данного компонента цифровых международных отношений, а также примеры использования методологии.

Методы анализа

Огромную роль в развитии цифровой дипломатии сыграла возможность использования различных компьютерных алгоритмов для исследования социальных сетей. Сегодня наблюдается бум в изучении внешней политики и дипломатии с точки зрения действий различных государств в киберпространстве.

Цифровая дипломатия требует использования особых методов анализа, которые относятся к изучению социальных сетей и поведению пользователей в сети Интернет. К самым распространенным можно отнести следующие: анализ хэштега (*hashtag tracking*), сетевой анализ (*network analysis*), сентимент-анализ (*sentiment analysis*) и анализ мнений и взглядов (*opinion analysis*).

Метод анализа хэштега дает ответ на вопрос о том, как развивается дискуссия по определенной теме, какие посты вызывают наибольший интерес и кто из участников обсуждения получает наибольшую популярность среди подписчиков.

Сетевой анализ выявляет ключевых блогеров и каналы международного вещания, которые создают информационный дискурс, шум и контекст вокруг определенной проблемы.

Сентимент-анализ или анализ тона текста оценивает реакцию пользователей на предлагаемые темы или информационные кампании, что способствует выявлению идентификации пользователей и их политической позиции.

Анализ мнений пользователей работает с текстами и осуществляет анализ часто употребляемых слов, терминов и эпитетов, что формирует знание о содержании постов и комментариев.

В последнее время набирает обороты кластерный анализ (или кластеризация) — это статистический метод, специализирующийся на классификации категорий, параметров и т.п. В области исследований международных отношений кластеризация может применяться для выявления идеологических позиций, идентификации кампаний цифровой дипломатии или для понимания структуры политического общения в социальных сетях. Классическими примерами выступают события в странах Северной Африки и на Ближнем Востоке в 2010-е гг. Используя указанные методы анализа, исследователи пришли к выводу, что Twitter^{*} сыграл определенную роль в информировании, организации и освещении акций протеста в стране, а в Ливии обычные офлайн-формы взаимодействия оказались значительно важнее для смены режима М. Каддафи.

В экспертном поле сформировалось две школы по анализу цифровой дипломатии: школа больших данных и школа малых данных. Большие данные подразумевают получение набора данных и их анализ машинным способом. К малым данным относятся ограниченное число постов, полученных из социальных сетей ручным или машинным способом. Долгое время ученые в области международных отношений использовали малые данные, что было приемлемым для изучения линейной цифровой дипломатии.

Используя ограниченное число твитов или постов, исследователи применяют приложения, такие как *SocioVizz*, *Netlytic*, *Netvizz*, *Popsters* и др., которые, однако, позволяют получить или проанализировать только ограниченное число постов. Однако многие исследования показывают, что интерпретацию полученных показателей необходимо

* Социальная сеть заблокирована в РФ. Доступ к сайту ограничен на основании статьи 15.3 федерального закона «Об информации, информационных технологиях и о защите информации».

осуществлять с учетом специфики политического и социокультурного контекста, в котором происходят действия пользователей.

Используя аналитику больших данных, специалисты пытаются ответить на вопросы эффективности цифровой дипломатии и политики вовлечения целевой аудитории. Однако, как и в случае работы с ограниченным сетом данных, мы должны понимать, что для формирования выводов требуются не только машинный анализ и анализ дискурса, но еще и понимание контекста (культурного и политического).

На смену понятию о цифровизации международных отношений и внешней политики пришла концепция о датафикации (*digitalization*). Датафикация — это использование больших данных и их аналитики в политических процессах. И особенностью современного развития данного феномена является бесконтрольное вовлечение аналитики различными государственными и негосударственными акторами. Сегодня самые разные участники международных отношений дипломатии, включая индивидуальных блогеров и огромные корпорации, государственные структуры, способны использовать данные социальных сетей для реализации политических и экономических интересов. Феномен датафикации меняет наше представление о больших данных. Опираясь на информацию социальных сетей, эксперты должны отличать «большие» данные от «малых», «обычных» или «огромных» данных в зависимости от количества и размера набора данных. Однако размер набора данных уже оказался недостаточным показателем. Поэтому в дипломатии используются дополнительные атрибуты «больших данных», например, их автоматическая генерация в режиме реального времени, полуструктурированные или неструктурированные атрибуты и, самое главное, возможности для обработки и анализа с помощью традиционных инструментов.

В итоге эксперты получают несколько видов аналитики — описательную, диагностическую, прогнозирующую или представительную, которая активно используется в практической области. Одним из примеров может выступать деятельность Центра глобального вовлечения США, который активно разрабатывает проекты дипломатии данных для противостояния информационной деятельности России в европейских государствах.

Изучению данных посвящена наука о данных (*data science*) — междисциплинарная область, которая использует научные методы, про-

цессы, алгоритмы и системы для извлечения знаний и понимания из многих структурированных и неструктурированных данных. Наука о данных находится на пересечении трех областей: математики, информатики и экспертизы предметной области. В данном случае предметная экспертиза — это сфера международных отношений или внешней политики США. Наука о данных — это концепт, охватывающий весь процесс сбора и обработки данных. Она включает в себя различные инструменты, статистику, алгоритмы и принципы машинного обучения для работы со сложными и большими наборами данных в контексте математики, статистики, компьютерных наук, информатики и экспертных знаний.

Однако исследователи, решившие обратиться к аналитике данных из социальных сетей, сталкиваются с определенными вызовами. Основной вызов — методика аккумуляции данных для исследования. Для этого используют встроенную аналитику для каждой из платформ социальных сетей, которая всё чаще и чаще является ограниченной и малодоступной, нативные приложения или прибегают к помощи программистов для создания особых алгоритмов сбора данных. Существует множество инструментов для анализа данных, но обычно выделяют два наиболее востребованных языка программирования: Python и R. Эти языки программирования популярны, поскольку относительно просты и поэтому чаще всего используются исследователями социальных наук во всем мире. Как правило, представителям нашей области знаний нужны самые простые программы (скрипты), которые выполняют серию команд для преобразования данных в форму, которая понятна для исследования. Кроме того, существуют различные инструменты сбора данных из социальных сетей. Как правило, многие из них имеют свободное фиксированное время использования или определенные бесплатные функции. Существует несколько бесплатных инструментов для сбора и анализа данных на разных языках программирования: например, StreamR на языке R и Tweepy на Python. Альтернативой может быть «Набор инструментов для сбора и анализа социальных сетей», созданного Амстердамским университетом, который использует набор инструментов для получения, сбора и анализа постов различными способами. Наконец, исследователи-международники используют способ извлечения данных из социальных сетей как веб-скрейпинг веб-страниц, который также

называется извлечением веб-данных и означает автоматический сбор данных с веб-сайта. Хотя языки программирования, такие как Python, и другие алгоритмы часто используются в области больших данных, существуют уже «готовые» продукты, которые были разработаны для предварительной обработки и анализа данных.

Особенности исследовательской работы с социальными сетями

Существует вызов при работе с большими данными в области дипломатии и внешней политики. Ситуация с доступностью данных социальных сетей постоянно меняется в связи с политической ситуацией. Достаточно вспомнить, как после знаменитых слушаний в конгрессе США в октябре 2017 по проблеме возможного вмешательства России в выборы США через социальные сети многие известные платформы ограничили доступ к сбору персональных сведений о пользователях. Или, например, такое популярное среди исследователей приложение, как *Netvizz*, теперь не может работать с некоторыми платформами, поскольку после скандала с *Cambridge Analytica* 2017 года, API (интерфейс программирования приложений) стал закрытой системой. Более того, общедоступные встроенные приложения на платформах делают невозможным повторение одного и того же сбора данных. Это является серьезным исследовательским ограничением, поскольку исследователи не знают о конкретных методах выборки, используемых публичными API для удовлетворения их потребностей.

Но на сегодняшний день Twitter* — один из важнейших источников «больших данных» из социальных сетей, доступный исследователям международных отношений, политики и дипломатии для сбора детализированных данных о взаимодействии людей во время локальных, региональных и глобальных событий. Более того, политика администрации платформы по формированию этики поведения и политики закрытия и приостановки функционирования различных аккаунтов, от фейковых до профайла президента США, создает новые интересные

* Социальная сеть заблокирована в РФ. Доступ к сайту ограничен на основании статьи 15.3 федерального закона «Об информации, информационных технологиях и о защите информации».

кейсы о цифровизации политики и о влиянии мнения администрации социальных сетей на качество и политическую окраску информационных потоков.

Цифровые следы, оставленные пользователями, данные об их взаимодействии друг с другом, а также различные переменные, такие как число подписчиков, избранное, язык, географическое положение и т.д., составляют интерес для исследователя. Как известно, социальная сеть учитывает использование пользователями других элементов, таких как прямые ответы на твиты (*replies*), обращения к другим аккаунтам (упоминания или *mentions*) и распространение информации (ретвиты или *retweets*). Взаимодействия, осуществляемые пользователями, выстраиваются в сети обсуждений под хэштегом, формируя диалоги и сообщества. Эти *хэштегированные* темы формируют, в свою очередь, вокруг себя сообщество пользователей, обсуждающих конкретные вопросы, и данный феномен носит название «феномен *issue publics*».

Другой вызов для использования анализа данных из социальных сетей — это предвзятость данных. Необходимо признать, что собранные данные, например из социальной сети составляют только до 1% от общего объема данных о каком-либо событии, что может сказаться на выводах исследователя. Исследователи также должны учитывать разницу в образовании, профессиональных занятиях, социальном статусе и прочем между пользователями платформы и населением в офлайне. «Граждане» Твиттера,** как правило, моложе и лучше образованы. Поэтому ограниченность собранных данных часто приводит к получению относительно достоверных выводах о глобальных событиях. Несмотря на широкое распространение социальных сетей, существует низкая представленность широкой публики в социальных сетях. Это влияет на репрезентативность данных. В некоторых странах широко используется одна платформа, в то время как в других популярна другая социальная сеть.

Еще важный момент об ограничениях получаемых данных из социальной сети можно назвать языковым вызовом (или языковой проблемой), создаваемой «языковыми пузырями», которые формируются

** Социальная сеть заблокирована в РФ. Доступ к сайту ограничен на основании статьи 15.3 федерального закона «Об информации, информационных технологиях и о защите информации».

пользователями, взаимодействующими на разных языках. При сборе данных всегда важно помнить о различиях хэштегов на разных языках, что также влияет на результаты исследования.

Однако даже если мир социальных сетей не идентичен миру офлайн, он полностью реален, потому что его пользователи, их желания, эмоции и политические взгляды реальны и оказывают масштабное влияние на всю систему международных отношений и дипломатии. Например, исследование дискурса вокруг выборов в Венесуэле полностью отразило офлайн-тенденции. Основываясь на анализе тысяч постов с геолокационными данными, эксперты точно предсказали электоральные тенденции в крупных городах Венесуэлы. Другими словами, обсуждения пользователей отражают политические предпочтения реальных людей, что является очень важной информацией для области исследований международных отношений. Таким образом, социальные сети могут быть объективным зеркалом реальности.

Извлечение данных состоит из трех этапов: сбор, анализ и визуализация данных. На первом этапе, который также можно назвать идентификацией данных, исследователь собирает информацию путем извлечения данных из одного или нескольких источников в социальных сетях и предварительной обработки. Предварительная обработка данных означает удаление ошибочных данных. Обычно собранные данные обозначаются «сырыми» и требуют предварительной обработки, чтобы очистить всё, что не нужно для исследовательских целей. Спам-твиты, боты для сетей фолловеров, языки и специальные символы должны быть отфильтрованы перед любым углубленным анализом.

Процесс выбора данных для анализа означает создание выборки данных (*sample*) для исследования, что связано с понятием переменных — количественных и категориальных данных. Планируя исследование, эксперты должны ответить на следующие вопросы: хронологический период для анализа; ключевое слово или хэштег для выбора данных; язык или языки данных; геолокация постов; атрибуты пользователей и др. Это только некоторые из вопросов, которые исследователь задает, прежде чем приступить к майнингу социальных сетей. На этапе анализа данных исследователь извлекает только релевантную информацию и структурирует, чтобы сделать ее более удобной для проведения исследований. Наконец, последний этап — это

интерпретация информации. На этом этапе данные визуализируются, чтобы продемонстрировать значение результатов.

Самое популярное направление касается изучения влияния поддельных новостей на информационное противостояние между государствами и другими международными акторами. Например, распространение «фейковых новостей» во время цикла президентских выборов в США в 2016 г. Сопоставив аккаунты с конкретными избирателями, можно выявить точное число граждан, кто подвергся влиянию «фейковых новостей», а кто распространял «фейковые новости». Были выявлены четыре группы сайтов: первая группа — общенациональные основные средства массовой информации; вторая группа — консервативная, третья — либеральная; и четвертая — все остальные. Фейковые новости были наиболее сконцентрированы среди консервативных избирателей. Анализ социальных сетей может выявить реальное отношение людей или крупных акторов к основным международным проблемам. Понимание этого отношения может позволить государствам и другим субъектам выбирать правильную стратегию или политику в отношении таких проблем.

Одна из главных задач, которая стоит перед исследователями-международниками, занимающимися аналитикой данных, — это как определить *влиятельных и активных пользователей*. Это важно как для понимания цифровой дипломатии, так и просто для практических задач по построению информационных цифровых кампаний. Постоянно появляются новые меры влияния, каждая из которых предлагает различные критерии измерения. Большое разнообразие критериев влияния включает в себя определение новых типов пользователей, которые тесно связаны с понятием «влиятельного пользователя».

Иногда влиятельных пользователей называют лидерами мнений или авторитетными участниками. Часто они ассоциированы с лучшими экспертами в конкретных областях. Некоторые исследователи различают лидеров мнений, инфлюенсеров и дискуссантов по типу деятельности и воздействия. Также выделяют «изобретателей» — пользователей, начинающих новую тему, и распространителей — пользователей, отвечающих за распространение этой темы. В другой классификации под распространителями понимаются пользователи, которые распространяют свое влияние, а также выделяются вовлекающие пользователи, которые способствуют взаимоотношениям с третьими сторона-

ми, и лидеры, т.е. ведущие распространяющие посредники. Можно распознать пользователей, предлагающих идеи (как правило, у них большое количество подписчиков), и соединителей (т.е. пользователей, соединяющих новичков), усилителей, кураторов, комментаторов и просто влиятельных наблюдателей.

Влиятельные пользователи также могут быть классифицированы в соответствии с их контентом и авторитетом. Общее мнение, что инфлюенсер имеет значительные показатели по фолловингу (т.е. подпискам) (F), ретвитам (RT), упоминаниям (M), ответам (RP) и лайков (FT).

До сих пор в науке о международных отношениях и в исследованиях по внешней политике доминирует мнение, что новостные сайты оказывают огромное влияние на другие средства массовой информации, которые публикуются не так часто, но на более широкую аудиторию. Тем не менее повестка дня в самой социальной сети формируется СМИ и журналистами, а не другими пользователями. Однако наши исследования с использованием больших данных показывают, что индивидуальные блогеры могут оказывать существенное влияние на политическую окраску содержания трендовых постов ответов.

Методика анализа хэштега или хэштеговой дипломатии всё еще остается значимым компонентом в изучении цифровой дипломатии или дипломатии данных США. Цифровая дипломатия имеет состязательный характер и является частью состязательной политики, поскольку является инструментом продвижения определенного содержания постов и сдерживания распространения постов своих противников. Однако обе стороны, как известно, могут использовать один и тот же хэштег, чтобы привлечь определенную часть пользователей на свою сторону. Политическая функция и значимость хэштегов еще только изучаются экспертами. Однако в практической плоскости дипломатия хэштега используется в цифровой дипломатии различных государств с 2010-х гг. Интересную оценку данному виду дипломатии дал Ричард Стенгель, заместитель госсекретаря по публичной дипломатии в период администрации Б. Обамы. Он отмечает, что дипломатия является наиболее эффективным инструментом для мобилизации пользователей в зарубежных странах вокруг определенных ценностей.

Хэштеги — это текстовые комбинации, перед которыми стоит «знак решетки» и которые используются для контекстной маркировки разго-

воров в интернете по определенной теме. Помимо маркировки, они также служат механизмом для создания и обмена темами; выражения ее поддержки; фильтрации и направления контента для определенной аудитории. Наконец, сам хэштег может быть сообщением или его частью. Хэштеги стали инструментом для запуска массовых кампаний и инструментом для онлайн-протеста и участия в политической жизни посредством «Хэштегового активизма», а также для распространения дезинформации и «фейковых новостей» в социальных сетях. Будучи мощными инструментами инфильтрации социальных сетей, хэштеги всё чаще используются конфликтующими или конкурирующими сторонами в политическом пространстве в глобальном масштабе, что заставляет исследователей больше концентрироваться на проблеме манипулирования трафиком в социальных сетях.

Многие исследования свидетельствуют, что выработалась определенная типология хэштегов, которые мобилизуют население, или предоставляют справочную информацию, или создают определенный функциональный фон. Например, анализ 2 млн твитов, связанных с бразильскими протестами июня 2013 г., показывает, что большинство используемых хэштегов были из разряда «волевых», как, например, *#ComeToTheStreet*. Такие хэштеги мобилизовали протестующих на активные действия. Особую популярность также приобрели справочные хэштеги — они информировали пользователей о местоположении событий (иногда это город или штат в Бразилии), а также обращались к международной аудитории для расширения информации о протестах. Наконец, выразительные или эмотивные хэштеги — это хэштеги, ориентированные на эмоции, мысли или мнения отправителя. Так, эта группа включала хэштеги, агрессивно нацеленные на экс-президента Бразилии Дилму Руссефф, — например, хэштег *#foradilma*.

Кейсы по анализу цифровой дипломатии

На примере работы официальных каналов цифровой дипломатии США, России и Китая в Афганистане и Сирии проиллюстрируем особенности, успехи и проблемы цифровой дипломатии. Были использованы данные разных временных периодов, включая данные по Афганистану в период с 2008 по конец 2018 г., по Сирии — в период с 2010 по 2017 г. Именно в эти различные промежутки времени

наблюдалась наибольшая активность цифровой дипломатии США, России и Китая в указанных странах, что было связано с решением политических задач.*

Для понимания ситуация в Афганистане и Сирии был использован один из самых простых, но не теряющий своей эффективности анализ — анализ хэштега. Анализ, как было указано, предполагает обработку всех постов с определенным хэштегом. В самом кратком изложении — были использовали все посты относительно определенного хэштега и определенной геолокации. Многочисленные посты официальных аккаунтов были извлечены из баз при помощи специальной компьютерной программы и последующей машинной обработки постов и комментариев.

Для поиска лидеров общественного мнения и влиятельных игроков были выбраны 250 самых влиятельных каналов за каждый месяц периода 2008–2018 гг.

Влиятельность постов или их информационный охват измеряется путем подсчета числа распространения информации пользователями или репостов, комментариев и построения кластеров маршрута репостов пользователей и их уровней. Другими словами, в современной цифровой дипломатии влиятельность — это масштаб взаимодействия команды дипломатов или индивидуальных блогеров с аудиторией, исчисляемый, как правило, числом репостов.

Используя машинный способ, были получены все доступные посты, содержащие определенный хэштег на английском и арабском языках, а также на дари, пушту и фарси, с веб-страницы расширенного поиска. С помощью языка программирования *Python* и запроса «SQL» в базу данных *Postgresql* была осуществлена классификация наиболее популярных постов и самых влиятельных аккаунтов в Twitter,** что позволило определить место правительственных аккаунтов разных стран, включая США, Россию и Китай, среди лидеров общественного мнения в изучаемых странах. Мы классифицировали популярность местных блогеров, различных радикальных организаций и пр. Особая роль была отведена географической локации блогеров, СМИ и прочих участников,

* Анализ был выполнен до блокировки социальной сети в РФ, в 2019–2020 гг.

** Социальная сеть заблокирована в РФ. Доступ к сайту ограничен на основании статьи 15.3 федерального закона «Об информации, информационных технологиях и о защите информации».

что позволило нам ранжировать наиболее значимые каналы или посты относительно их географической принадлежности и сделать вывод о влиянии местных или зарубежных блогеров или СМИ на пользователей в Афганистане и Сирии.

Результаты анализа предоставляют ответ на самый важный вопрос: оказывает ли влияние официальная цифровая дипломатия в виде деятельности официальных аккаунтов и каналов международного вещания на цифровое пространство? Или отдельные группы, блогеры и неофициальные каналы оказывают большее влияние и снижают эффективность распространения информационных постов официальных каналов?

Пример Афганистана

Афганистан показывает эволюцию цифровой дипломатии самых различных акторов. Только в 2011–2012 гг. афганские пользователи обратили внимание на твиты военных ведомств США, а также на твиты международных организаций. В афганском сегменте Твиттера*** появились аккаунты МИД, таких как Госдепартамент США и МИД РФ, которым удавалось захватывать внимание афганцев. А вот период 2013–2015 гг. — это время многообразия каналов международного вещания США, России, Китая, Саудовской Аравии в афганском сегменте социальных сетей. Индивидуальные блогеры с западной повесткой также занимали ведущие места. Как оказалось, посты одного из афганских известных блогеров и музыкантов, выпускника Американского университета в Шардже, были более популярными и влиятельными, чем все посты каналов международного вещания правительства США, России, КНР и т.д. Судя по нашим данным, блогер удерживал первенство на протяжении нескольких лет, до конца 2016 г., после чего его посты стали менее популярными, чем посты радикальных групп и всех тех, кто вел борьбу против коалиционных войск.

Данный пример объясняет одну из сторон феномена датафикации в международных отношениях в части роли влияния индивидуальных акторов на политику. Привлечение блогеров с дружественной

*** Социальная сеть заблокирована в РФ. Доступ к сайту ограничен на основании статьи 15.3 федерального закона «Об информации, информационных технологиях и о защите информации».

позицией на сторону определенной государственной цифровой дипломатии является значимой частью современной системы международных отношений. Однако подобное применение требует постоянного вовлечения индивидуальных лиц в информационный дискурс правительственной позиции.

МИДы и каналы международного вещания США, России и КНР также имели некоторое влияние на пользователей, особенно если твиты касались проектов по развитию Афганистана. Исследование показало, что между странами, такими как Саудовская Аравия, Иран, Россия, Китай, США, развернулась борьба за лидерство в информационном пространстве Афганистана. Анализ содержания постов показывает, что посты о проектах по развитию Афганистана или, например, об акциях США вызывали наибольший интерес и активно цитировались афганцами. Активные пользователи позитивно реагируют на посты США, РФ и других стран, которые связаны с проблемой развития и восстановления Афганистана, а также с проведением экономических реформ. США создали больше всех официальных каналов вещания в Афганистане, включая местный телеканал @TOLOnews, до сих пор вещающий в Кабуле. Канал очень быстро отвоевывал аудиторию социальных сетей. Твиты канала всегда пользовались популярностью среди населения. Однако традиционные каналы вещания, созданные специально с пропагандистскими целями, не получали у афганцев той поддержки, на которую рассчитывали США. Совсем не был популярен канал США, созданный специально для противостояния радикальным группам в приграничных районах Афганистана и Пакистана как Radio Deewa.

Но на снижение эффективности цифровой дипломатии государств в афганском сегменте интернета оказывала влияние активная информационная политика местных групп талибов и других внешних игроков. Как только «цифровые дипломаты» США или других стран по каким-то причинам прекращали создавать контент в социальных сетях или международное вещание в Афганистане не распространяло привлекательных лозунгов, информационный вакуум быстро заполнялся информацией, идущей от группы экстремистов, медиа-джихадистов и т.п. Очень быстро позитивная повестка сменялась негативными постами о коалиционных силах и США, особенно если в Афганистане случались кризисные ситуации. Анализ показал, что информация всех внешних игроков проигрывала на фоне информации, идущей

от местных блогеров или каналов, далеко не дружественных в отношении зарубежных стран и игроков. *Таблица 1* показывает рейтинг 250 наиболее влиятельных аккаунтов в апреле 2018 г.

Таблица 1

Расстановка каналов цифровой дипломатии в Афганистане в апреле 2018 г.

Место	Каналы цифровой дипломатии
1	Канал заблокирован
2	Канал заблокирован
3	Канал заблокирован
42	U.S. Dept of Defense
46	Department of State
119	TOLOnews
129	Pakistan Defence Command
154	Sputnik (Russia)
164	Govt of Pakistan
213	U.S. Central Command
220	RT

Из *Таблицы 1* следует, что ведущие места заняли посты аккаунтов, которые позже были удалены администрацией Twitter.* Более того, места в рейтинге между указанными каналами также занимали твиты с чувствительной информацией. Но в тот период эти посты были доступны афганским пользователям и цитировались широко по сети.

Зарубежные каналы вещания США, России или КНР не могли или не имели интенцией противостоять информации или информационным кампаниям в силу проведения разобщенной цифровой дипломатии. Указанные каналы вещания продвигали внешнеполитические цели своих государств, при этом вступая в противоречие с конкурентами

* Социальная сеть заблокирована в РФ. Доступ к сайту ограничен на основании статьи 15.3 федерального закона «Об информации, информационных технологиях и о защите информации».

из других стран, что, несомненно, было только на руку радикальным информационным группировкам в Афганистане.

Кейс по Афганистану свидетельствует о двух чертах современного процесса датафикации. С одной стороны, официальная цифровая дипломатия может быть легко осаждена многочисленными блогерами и их повесткой. Это и есть цифровая неопределенность датафикации — мы не можем быть готовы к информационной кампании, которая удачно попадет в аспирации пользователей. С другой стороны, эффективность цифровой дипломатии государств можно увеличивать за счет привлечения на свою сторону индивидуальных блогеров, а также посредством постоянного создания популярного контента. В свою очередь, популярный контент и притягательные краткий лозунг или информация могут быть созданы с помощью специальных алгоритмов, которые на основе анализа и интерпретации постов пользователей, а также анализа их предпочтений и пр., будут способны генерировать новые сообщения, что является одной из областей применения искусственного интеллекта.

Пример по Сирии

По второму кейсу был произведен анализ больших данных по хэштегу «Сирия» на английском и арабском языках, а при помощи специального созданного программного алгоритма было собрано более 34 млн твитов и постов и осуществлена классификация наиболее влиятельных твитов за каждый месяц и самых влиятельных аккаунтов с 2010 по 2017 г. Именно в 2010 г. стали появляться первые местные и региональные игроки в цифровом пространстве Сирии с определенной политической повесткой, в основном оппозиционной, а 2017 г. стал первым годом некоторой популярности зарубежных каналов вещания таких стран, как США и Россия. Выбранный промежуток времени показывает особенности цифровой дипломатии США, России и Китая в Сирии.

Выводы полностью опровергли эффективность так называемой линейной цифровой дипломатии, что активная деятельность официальных каналов в другой стране должна привести в активизации и популярности постов цифровой дипломатии. Оказалось, что не западные и не российские каналы международного вещания или блогеры оказывали определяющее влияние на умы сирийских граждан. Местные блогеры и региональные державы, включая Саудовскую Аравию,

ее каналы международного вещания, а также многочисленная армия частных блогеров этой страны были в числе лидеров по формированию информационного и политического дискурса о Сирии.

Были выявлены самые популярные каналы среди сирийских пользователей в 2013 г. Мы использовали 2013 г., поскольку именно тогда впервые среди арабских блогеров и каналов вещания Саудовской Аравии, религиозных мыслителей и исламистов стали пробиваться западные каналы вещания. Но эти каналы вещания не включены официально в инструментарий государственной цифровой дипломатии. Оказалось, что местные блогеры, оппозиционеры, официальные СМИ Саудовской Аравии и каналы, которые позже будут официально закрыты самим правительством Саудовской Аравии из-за радикальной религиозной риторики (например, цифровой телеканал Wesal TV), держали внимание сирийских пользователей. Большинство твитов были на арабском языке, и здесь необходимо отметить, что Сирия кардинально отличалась, скажем, от Афганистана или Ирана в отношении доминирования языка социальных сетей. Арабский язык доминировал. Западные СМИ, которые не являются частью официальной цифровой дипломатии США и Великобритании, первыми захватили внимание пользователей, но находились внизу рейтинга и не всегда удерживались даже в рейтинге двухсот пятидесяти популярных каналов.

Анализ показывает, что до 2014–2015 гг. среди авторов популярных постов не было каналов США, России или международных организаций. Но даже когда ситуация стала меняться, цифровая дипломатия США, России или Китая терялась на фоне информации, идущей от блогеров и каналов международного вещания Саудовской Аравии, Кувейта, а также на фоне постов популярных блогеров, многие из которых были позже заблокированы из-за информации радикального толка.

В течение последующего периода 2015–2018 гг. картина социальных медиа в Сирии изменилась. Каналы цифровой дипломатии США, России и других стран добились некоторого внимания сирийских пользователей. Однако зарубежные каналы не пользовались такой популярностью, как региональные блогеры или каналы вещания Саудовской Аравии. Каналы международного вещания и цифровой дипломатии США и России, в отличие от каналов Китая, получали внимание среди пользователей в 2017 г. Все другие позиции распределились между блогерами, оппозиционерами, радикальными исламистами, а также СМИ

Саудовской Аравии. Однако популярность каналов США или России была краткосрочной и быстро улетучилась. В последующие месяцы и годы ни США, ни РФ, ни другие каналы глобального вещания не входили в первые 250 самых цитируемых каналов.

Кейс по Сирии свидетельствует, что официальная цифровая дипломатия может долгое время оставаться неэффективной с точки зрения привлечения внимания целевой аудитории в зарубежных странах по причине наличия сильных региональных игроков, СМИ и блогеров, которые не сотрудничают с официальными каналами. Например, в Сирии особую популярность получили блогеры и СМИ Саудовской Аравии, а не каналы вещания США или России. Именно они держали под контролем повестку, формировали фрейм, в котором шли политические дискуссии. Такая ситуация затрудняет работу цифровой дипломатии, но повышение эффективности возможно при наличии кризисных ситуаций, в которых информация (пост) той или иной страны становится востребованной.

Примеры по Афганистану и Сирии свидетельствуют, что цифровая дипломатия государств может быть менее эффективной, чем цифровая активность таких участников цифровой дискуссии, как индивидуальные блогеры, СМИ или селебрити. В любой момент отдельный пост или цифровая акция могут ликвидировать все усилия каналов международного вещания. Эта неопределенность преодолима при помощи постоянного мониторинга цифрового пространства на предмет роста популярности каких-то стейкхолдеров и возможного партнерства с ними по решению отдельной политической задачи. Пример Афганистана в этом отношении показателен: несколько лет афганскому блогеру прозападной ориентации удавалось завладеть вниманием пользователей. Фрагментированность является большей проблемой, и казалось бы, она преодолима посредством расширения числа участников и фильтрации искусственно созданных кампаний. Однако пример Сирии показывает, что не так просто каналам цифровой дипломатии, например США или России, преодолеть привычную ориентацию пользователей на местные или региональные каналы Саудовской Аравии.

Однако для успешной реализации цифровой дипломатии требуются постоянная аналитика больших данных и использование специальных алгоритмов для продвижения информации. Наконец, приоритеты внешней политики оказывают влияние на активность каналов цифровой

дипломатии. Пример Китая свидетельствует, что Сирия выпадала из значимых приоритетов внешней политики Пекина, и поэтому китайские каналы не проводили активную информационную деятельность. А вот в Афганистане — в социальных сетях — Китай присутствовал, но не так активно, как США или Россия.

Вопросы и аналитические задания

1. На основании следующей литературы систематизируйте актуальные методы цифровой дипломатии:
 - *Bjola C. Cyber-Intelligence and Diplomacy: the Secret Link // Secret Diplomacy: Concepts, Contexts and Cases. Bjola C., Murray S. (Eds.). N.Y.: Routledge. P. 201–228.*
 - *Fjällhed A. Managing Disinformation Through Public Diplomacy // Public Diplomacy and the Politics of Uncertainty. Surowiec P., Manor I. (Eds.). L.: Palgrave MacMillan, 2019. P. 227–253.*
 - *Manor I. The Russians are Laughing! The Russians are Laughing! How Russian Diplomats Employ Humour in Online Public Diplomacy // Global Society. 202. Vol. 35 (1). P. 61–83.*
 - *Manor I., Bjola C. Public Diplomacy in the Age of ‘Post-Reality’ // Public Diplomacy and the Politics of Uncertainty. Surowiec P., Manor I. (Eds.). L.: Palgrave MacMillan, 2019. P. 111–143.*
 - *Manor I., Pamment J. From Gagarin to Sputnik: the Role of Nostalgia in Russian Public Diplomacy // Place Branding and Public Diplomacy. 2022. Vol. 18. P. 44–48.*
 - *Tsvetkova N. Russian Digital Diplomacy: A Rising Cyber Soft Power? // Russia’s Public Diplomacy. Studies in Diplomacy and International Relations. Velikaya A., Simons G. (Eds.). Cham: Palgrave Macmillan. P. 103–117.*
 - *Wu Y. From External Propaganda to Mediated Public Diplomacy: The Construction of the Chinese Dream in President Xi Jinping’s New Year Speeches // Public Diplomacy and the Politics of Uncertainty. Surowiec P., Manor I. (Eds.). Cham: Palgrave Macmillan, 2021. P. 29–55.*
2. Чем отличаются научные подходы к анализу больших данных и малых данных?
3. Охарактеризуйте применение доступных средств программирования для понимания цифровой дипломатии.

Рекомендованная литература

1. *Bruns A., Highfield T., & Burgess J.* The Arab Spring and Social Media Audiences: English and Arabic Twitter Users and Their Networks. *American Behavioral Scientist*. 2013. Vol. 57 (7). P. 871–898.
2. *Jacobson B. R., Höne K. E., Kurbalija J.* Data diplomacy. Updating diplomacy to the Big Data Era // DiploFoundation, 2018. https://www.diplomacy.edu/sites/default/files/Data_Diplomacy_Report_2018.pdf.
3. *Manor I.* The Digitalization of Diplomacy: Toward Clarification of a Fractured Terminology. Working Paper № 2. Oxford Digital Diplomacy Research Group, 2018.
4. *Ruiz-Soler J.* Twitter Research for Social Scientists: a Brief Introduction to the Benefits, Limitations and Tools for Analysing Twitter data // *Revista Dígitos*, 3. 2017. <https://revistadigitos.com/index.php/digitos/article/view/87>.
5. *Tsvetkova N.* Russian Digital Diplomacy: A Rising Cyber Soft Power? // *Russia's Public Diplomacy. Studies in Diplomacy and International Relations*. Velikaya A., Simons G. (eds.). Cham: Palgrave Macmillan. P. 103–117.

Т е м ы д л я с е м и н а р с к и х з а н я т и й

Линейная дипломатия государств на примере МИД.

Дипломатия алгоритмов: негосударственные акторы в социальных сетях.

Анализ «малых данных»: цифровая дипломатия США на платформе Telegram.

Развитие института кибердипломатии.

Анализ больших данных: конфликты в Сирии, Афганистане, Украине.

Цифровая мощь отдельных государств: аппарат, стратегии и кейсы.

Новые инструменты для анализа социальных сетей и цифровой дипломатии.

Киберсуверенитеты и политика продвижения технологических норм: США, Китай.

Глобальное управление интернетом: дебаты и соглашения в ООН.

Двухсторонние отношения в области кибербезопасности.

Рекомендуемая литература

1. *Bjola C., Zaiotti R.* Digital Diplomacy and International Organizations. Autonomy, Legitimacy and Contestation. L.: Routledge, 2021.
2. *Manor I., Bjola C.* Public Diplomacy in the Age of 'Post-Reality' // Public Diplomacy and the Politics of Uncertainty. Surowiec P., Manor I. (Eds.). L.: Palgrave MacMillan, 2019. P. 111–143.
3. *Manor I.* The Digitalization of Public Diplomacy. L.: Palgrave Macmillan, 2021.
4. *Stadnik I.* Internet Governance in Russia — Sovereign Basics for Independent Runet, 2019 // SSRN. <https://ssrn.com/abstract=3421984>.
5. *Stadnik I.* *Sovereign RUnet: What Does it Mean?* // Internet Governance Project, Georgia Institute of Technology, 2019. <https://www.internetgovernance.org/research/sovereign-runet-what-does-it-mean/>.
6. *Stadnik I.* What is cybersecurity regime and how we can achieve it? // Masaryk Journal of Law and Technology. 2017. Vol. 11 (1). P. 129–154.
7. *Sytnik A.* Digitalization of Diplomacy in Global Politics on the Example of 2019 Venezuelan Presidential Crisis // Digital Transformation and Global Society. Vol 1038. Springer: Cham, 2019.
8. *Tsvetkova N., Sytnik A., Grishanina T.* Digital International Relations: Uncertainty, Fragmentation, and Political Framing // The Routledge Handbook of Russian International Relations Studies. Lagutina M., Tsvetkova N., Sergunin A. (Eds.) N.Y., L.: Routledge, 2023. P. 381–395.
9. *Tsvetkova N., Sytnik A.* Venezuela in U.S. Public Diplomacy, 1950s-2000s: The Cold War, Democratization, and the Digitalization of Politics // Cogent Social Sciences. 2019. Vol. 5 (1). P. 1–15.
10. *Tsvetkova N., Yarygin G.* Sprawling in Cyberspace: Barack Obama's Legacy in Public Diplomacy and Strategic Communication // *Journal of Political Marketing*. 2020. Vol. 1. P. 5–20.
11. *Tsvetkova N.* Dealing with a Resurgent Russia: Engagement and Deterrence in US International Broadcasting, 2013–2019 // *Vestnik of St. Petersburg State University. International relations*. Vol. 4. 2019. P. 435–449.
12. *Tsvetkova N.* Soft Power and Public Diplomacy // *Russia and the World: Understanding International Relations*. Tsvetkova. N. (Ed.), Lanham, N.Y., L.: Roman & Littlefield, 2017. P. 231–251.

13. *Tsvetkova N.* Russian Digital Diplomacy: A Rising Cyber Soft Power? In *Russia's Public Diplomacy: Evolution and Practice*. Velikaya A., Simons G. (Eds.). L.: Palgrave Macmillan, 2019. P. 103–117.
14. *Лебедева М. М., Зиновьева Е. С.* Технология международных переговоров в цифровую эпоху. М.: Аспект-пресс, 2022.
15. *Стадник И., Цветкова Н.* Политика кибербезопасности США // *Международные процессы*. 2018. Т. 16. № 3 (54). С. 157–169.
16. *Стадник И. Т.* IGF поднимает проблему цифрового изоляционизма // РСМД. <https://russiancouncil.ru/analytics-and-comments/analytics/igf-podnimaet-problemu-tsifrovogo-izolyatsionizma>.
17. *Сучков М. А.* «Геополитика технологий»: международные отношения в эпоху Четвертой промышленной революции // *Вестник Санкт-Петербургского университета. Международные отношения*. 2022. № 2. С. 138–157.
18. *Цветкова Н. А.* Дипломатия данных США: цели, механизм, содержание // *США и Канада: экономика, политика, культура*. 2020. № 9. С. 104–116.
19. *Цветкова Н. А.* Цифровая дипломатия: феномен в международных отношениях и методология изучения // *Вестник РГГУ. Серия. Международные отношения*. 2020. № 2. С. 37–37.
20. *Цветкова Н. А., Сытник А. Н.* Информационные технологии в реалиях политического кризиса: от сетевого проекта «Евромайдан» до создания стратегической коммуникации на Украине (2013–2016 гг.) // *Власть*. 2017. Т. 25. № 4. С. 86–91.
21. *Цветкова Н. А., Сытник А. Н.* Публичная дипломатия в Афганистане, 2002–2018 гг.: влияние США на социальные сети, политическую систему и университеты // *Вестник Санкт-Петербургского университета. Политология. Международные отношения*. 2018. Т. 11. № 4. С. 344–361.
22. *Цветкова Н. А., Сытник А. Н., Гришанина Т. А.* Цифровая дипломатия и digital international relations: вызовы и новые возможности // *Вестник Санкт-Петербургского университета. Международные отношения*. 2022. № 2. С. 174–196.
23. *Ярыгин Г. О.* Электронное и интернет-голосование в избирательном процессе США // *США и Канада: экономика, политика, культура*. 2016. № 9 (561). С. 90–104.

Сведения об авторе:

Цветкова Наталья Александровна — профессор, завкафедрой американских исследований, Санкт-Петербургский государственный университет.

Учебное издание

Цветкова Наталья Александровна

Цифровые инструменты в международной политике:
содержание и методы анализа

Учебно-методическое пособие

Подписано к публикации 22.07.2023.

Формат 60×90/16. Усл. печ. л. 3,5.

Заказ 14624.