



CYBER DIPLOMACY ON THE AXIS OF DIGITAL TRANSFORMATION

N. A. Kasimova

*Doctor of political sciences, professor
Tashkent State University of Oriental Studies
Tashkent, Uzbekistan*

M. N. Ergashbaev

*Master's student
Tashkent State University of Oriental Studies
Tashkent, Uzbekistan*

ABOUT ARTICLE

Key words: cyberspace, diplomacy, digital world, cybersecurity, cyberattacks, globalization, international organizations.

Received: 11.05.23

Accepted: 13.05.23

Published: 15.05.23

Abstract: The article analyzes the increasing role of digital technologies and the Internet in the foreign policy of states in the context of globalization. The activity of actors of international relations in cyberspace is investigated.

RAQAMLI TRANSFORMATSIYA O'QIDA KIBER DIPLOMATIYA

N. A. Qosimova

*Siyosiy fanlar doktori, professor
Toshkent davlat sharqshunoslik universiteti
Toshkent, O'zbekiston*

M. N. Ergashboev

*Magistratura talabasi
Toshkent davlat sharqshunoslik universiteti
Toshkent, O'zbekiston*

MAQOLA HAQIDA

Kalit so'zlar: kibermakon, diplomatiya, raqamli dunyo, kiberxavfsizlik, kiberhujumlar, globallashuv, xalqaro tashkilotlar.

Annotatsiya: Maqolada globallashuv sharoitida davlatlarning tashqi siyosatida raqamli texnologiyalar va internetning ortib borayotgan roli tahlil qilinadi. Xalqaro munosabatlar subyektlarining kibermakondagi faoliyati o'rganiladi.

Global kiberxavfsizlikning dolzarb masalalari ko'rib chiqiladi.

КИБЕРДИПЛОМАТИЯ НА ОСИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ**Н. А. Касимова***Доктор политических наук, профессор**Ташкентского государственного университета востоковедения**Ташкент, Узбекистан***М. Н. Ергашибаев***Студент магистратуры**Ташкентский государственный университет востоковедения**Ташкент, Узбекистан*

О СТАТЬЕ

Ключевые слова: киберпространство, дипломатия, цифровой мир, кибербезопасность, кибератаки, глобализация, международные организации.

Аннотация: В статье анализируется возрастающая роль цифровых технологий и интернета, во внешней политике государств в условиях глобализации. Исследуется деятельность субъектов международных отношений в киберпространстве.

Рассмотрены актуальные вопросы глобальной кибербезопасности.

ВВЕДЕНИЕ

Важные события в истории не только привели к быстрым изменениям мирового порядка, но и заложили основу для изменения содержания дипломатии. Сегодня информационные и коммуникационные технологии, которые стали важной частью международных отношений, с каждым днем усиливают свое влияние и в то же время демонстрируют свою компетентность в киберпространстве. Информационные и коммуникационные технологии, которые облегчают обмен информацией, создают важные инфраструктурные услуги для граждан и делают возможным их повседневное взаимодействие, быстро стали важным инструментом на основе международных отношений. В этом контексте «кибердипломатия», возникшая как новая концепция с эффектом цифровизации, олицетворяет силу информации и технологий в политике.

ОСНОВНАЯ ЧАСТЬ

Если рассматривать кибердипломатию как концепцию, она определяется как активная часть киберпространства, в рамках дипломатических инструментов и идей, ориентированная на решение проблем в киберпространстве. В этом контексте дипломатия сформировалась как новый революционный метод, и впоследствии изменилось и ее содержание. В эту эпоху, когда преобладает цифровизация, рост числа пользователей интернета и прозрачное распространение их информации и мыслей на этой платформе, стало показателем перехода к новой модели, ориентированной на сообщества [1].

Обычно правительства и международные организации используют интернет и социальные сети для легкого достижения стратегических целей во внешней политике. Таким образом, решение дипломатических вопросов через Интернет и использование технических средств коммуникации и выработка решений в этой области является результатом цифровизации. Возможность взаимодействия через Интернет и информационные системы также способствует международной дипломатической деятельности. Многие правительства во всем мире активно используют важные инструменты социальных сетей и на их основе формируют свои внешнеполитические программы.

Технологическая революция вызванная глобализацией, сделала дипломатию частью перемен и сумела адаптировать дипломатов к этой сфере. Сегодня в силу своих обязанностей дипломаты должны ежедневно следить за СМИ и событиями. На этом этапе дипломаты могут легко оценивать события со всех сторон благодаря интернету, который облегчает их работу [2]. По этой причине быстрое развитие интернет-технологий, которые являются строительным блоком изменений, заставило дипломатов повысить свою компетентность в цифровой платформе.

Социальные сети потенциально могут изменить контекст международных отношений. По этой причине использование социальных сетей в дипломатических отношениях помогает дипломатам выполнять множество действий, от международных переговоров до урегулирования кризисов. Все это составляет дорожную карту для понимания глобальной безопасности и дипломатии XXI века. Таким образом, правительства доминирующие в цифровом мире, получают преимущество в киберпространстве по сравнению с бездействующими правительствами.

Небезопасность киберплатформ изо дня в день раскрывает концепцию кибердипломатии. Хотя цифровая дипломатия и кибердипломатия связаны друг с другом, концептуально они различаются. Цифровая дипломатия - это перенос всей дипломатической деятельности на цифровую платформу. В этом контексте цифровая дипломатия направлена на повышение репутации страны и реализацию ее внешнеполитических целей путем общения с гражданами. Путь к достижению этой цели - подключиться к цифровым инструментам. Кибердипломатия, с другой стороны, направлена на разработку дипломатических стратегий соразмерно угрозам в кибермире.

Если привести пример всех этих событий, то можно поставить Израиль на первое место в этой области. Потому что Израиль - одна из стран, наиболее активно и эффективно использующих кибердипломатию. Хайфский университет в Израиле запустил программу обучения «дипломатов-граждан». В рамках этой программы проводятся тренинги по

качеству комментариев в интернет-газетах, вводу и обновлению информации на страницах Википедии, форумах, а также использованию Facebook и Twitter. Таким образом, программа направлена на то, чтобы гражданские дипломаты стали доминировать в виртуальной среде.

Другая страна, Австралия, назначила в 2016 году «посла по киберпространству», чтобы создать безопасную и прозрачную интернет-среду для своих международных партнеров. Его цель здесь - представить страну в международном киберпространстве [3].

Понятие «киберпространство» было впервые использовано Луи Куффиньялом в 1958 году, а в 1984 году этот термин был использован Уильямом Гибсоном в романе «Нейромант» и автор стал пионером общего распространения этой концепции [4]. Кибербезопасность привлекает к себе внимание с точки зрения безопасности, которая является одним из рабочих направлений международных отношений, а также имеет место в дискуссиях по международному праву.

25 декабря 2015 года президент США Барак Обама и президент Китая Си Цзиньпин пришли к взаимному соглашению о том, что обе стороны «не будут проводить кибератаки, связанные с нарушением авторских прав и кражей в Интернете, и не будут поддерживать лиц и организации, которые сознательно проводят кибератаки».

Хотя некоторые рассматривали это соглашение как важный шаг, многие аналитики оценили его как соглашение, которое останется на бумаге. Учитывая, что киберпространство имеет свою собственную природу неопределенности и анархии, вопрос о том, является ли соглашение, которое останется на бумаге, может быть включен в более реалистичные рамки. Китай считается одним из самых агрессивных игроков в киберпространстве. Точно так же это одна из основных причин, лежащих в основе соглашения США с Китаем. Согласно докладу, представленному в Палате представителей США в 2013 году, утверждалось, что разведывательная деятельность Китая была нацелена на военную и экономическую инфраструктуру США, украдала экономику, технологические инновации и авторские права и в то же время получила доступ к военным секретам. В отчете указывалось, что ежегодно против Министерства обороны США совершается 50 000 атак и что ведущей страной атак был Китай [5].

Достижения науки и техники в нашем веке также повлияли на измерения безопасности. Обычные элементы безопасности уступили свое место асимметричным элементам и вызвали дискуссии в восприятии безопасности. Самым большим преимуществом кибер-мира является то, что кибероружие дешевле обычного оружия, преступника нелегко обнаружить, а действия в киберпространстве могут иметь разрушительные последствия в реальном мире. Организация Объединенных Наций (ООН)

работает над кибербезопасностью с 1980 года. Исследования по кибербезопасности проводятся в основном на основе резолюций Генеральной Ассамблеи ООН через агентство ООН, МСЭ (Международный союз электросвязи). В ООН также работает Межправительственная группа экспертов по киберпреступности, и есть оценки, что эта инициатива будет более всеобъемлющей и проложит путь к международным нормам мирного использования киберпространства в будущем [6].

Роль платформ социальных сетей в цифровой дипломатии

Основа цифровых медиа, несомненно, формируется вокруг оси социальных медиа. «Социальные сети» - это термин, обычно используемый для онлайн-инструментов и веб-сайтов, которые создают взаимодействие, предоставляя пользователям возможность делиться информацией, мыслями, интересами и знаниями. Различные веб-сайты и приложения (twitter, facebook, instagram, youtube и т. д.) сделали цифровую среду привлекательной. Социальные сети стали неотъемлемой частью жизни везде, где есть доступ в Интернет.

С точки зрения дипломатии, в новую эпоху сбор информации осуществляется через социальные сети, микроблоги и поисковые системы. В настоящее время Интернет рассматривается государствами, как уникальный дипломатический инструмент; таким образом, государства имеют возможность продвигать не только свою позицию по различным вопросам, но и свои идеи по всему миру, благодаря целенаправленному использованию интернета. Однако социальные сети сопряжены с множеством рисков для государств. Социальные сети дают людям возможность объединяться с определенной целью из разных частей мира, и это сделало политику государств гораздо более заметной, чем раньше. Таким образом, локальное событие может легко оказать глобальное влияние.

В контексте дипломатических отношений Twitter занял важное место в социальных сетях. Настолько, что Twitter недавно стал рассматриваться как эффективный инструмент связей с общественностью. Через Twitter правительства или учреждения взаимодействуют со своими подписчиками индивидуально. Twitter обеспечивает взаимодействие между государствами и гражданами и прокладывает путь для формирования Twitter дипломатии, внося большой вклад в политическое участие граждан [7].

С точки зрения официальных учреждений Twitter, который вышел на первый план в социальных движениях, таких как Арабская весна и события в Гези, привнес новое измерение в отношения с гражданами. Мысли граждан или общественных организаций, можно мгновенно измерить через этот канал и соответствующие действия могут быть предприняты.

Дипломатические угрозы и атаки в киберпространстве

Последовательные технологические разработки в информационную эпоху также изменили размер и методы войн. Таким образом, государства начали становиться еще сильнее на международной арене, чтобы не подвергаться кибератакам или минимизировать эти атаки. Однако страны, которые часто используют киберактивность, не очень умеренно смотрят на формирование глобальной кибербезопасности. В этом контексте угроза кибервойны в цифровом мире проявляется на международной арене. Государства могут по-разному использовать тактические элементы в стратегических кибервойнах. С другой стороны, атакованный субъект может дифференцировать масштаб конфликта за счет взаимной эскалации. В этом случае очень важным становится вопрос о пределах кибервойны. Рассмотрение методов атаки как возможности второго удара в кибервойнах - важная проблема ближайшего будущего. Должно быть четко определено административно, будут ли дипломатические преференции использоваться обеими сторонами или будут предприняты шаги в рамках антикризисного управления [8].

В свете всей этой информации, основной темой становится необходимость безопасного и глобального сотрудничества между государствами, поскольку страны используют свой баланс сил, как козырную карту друг против друга на киберплатформе. Увеличение количества правовых норм и институтов кибербезопасности важны для создания глобальной зоны кибербезопасности, чтобы поддерживать среду взаимного доверия, мира и минимизировать угрозы в киберпространстве.

ЗАКЛЮЧЕНИЕ

Развитие цифровой дипломатии выявило необходимость кибердипломатии. Цифровая дипломатия играет важную роль в переводе дипломатической деятельности на цифровую платформу. Например: Дипломатические переговоры ведутся через платформу Zoom, соглашения заключаются в электронном виде и т. д. государства активно используют множество различных платформ и приложений.

Однако использование дипломатии на цифровых платформах может вызвать проблемы. Потому что к цифровым платформам может получить доступ каждый. Таким образом, цифровые платформы становятся небезопасными, поскольку они день ото дня подвергаются серьезному риску. Эта ситуация показывает важность кибердипломатии. Кибердипломатия - это способность государств безопасно осуществлять свою дипломатическую деятельность и отношения на киберплатформе, очищая цифровые платформы от всех возможных опасностей. Для этого необходимо сближение государств в рамках сотрудничества. Важность этого сотрудничества совершенно очевидна в

современном мире, где цифровизация ускоряется. Государствам необходимо предпринять решительные шаги в этой области для предотвращения возможных киберугроз и атак.

Киберпространство – явление выходящее за пределы национальных границ, и показывает насколько важны международные организации, межгосударственная солидарность и сотрудничество на ограниченной территории. В этом контексте кибердипломатия потребует от государств объединения, чтобы обеспечить безопасность в киберпространстве.

Причину, по которой кибербезопасность и киберпространство так тесно переплетаются с международными отношениями, можно рассматривать как возможность для «исследований безопасности» и «развития военного потенциала». Китайская Народная Республика была включена в космическое соревнование между США и Россией в период холодной войны. В конце концов очевидно, что государствам трудно или даже утопично достичь консенсуса в области киберпространства. Однако точка зрения, которая может быть выдвинута для установления мира, заключается в создании платформ киберпроблем в глобальном масштабе. Таким образом, не исключено, что международные организации и субъекты, играющие ведущие роли в киберпространстве, могут встретиться на общей почве.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Bjola, C., M. Holmes (2015). Digital Diplomacy: Theory and Practice, Newyork: Routledge. pg. 25-28
2. Tuncer, H. (2006). Küresel diplomasi, Ankara: Ümit Yayıncılık. s.13.
3. Sandre, A. (2015). Digital diplomacy: Conversations on Innovation in Foreign Policy, Digital Diplomacy: Theory and Practice, Newyork: Routledge pg. 105
4. KORHAN Sevda, Siber Uzayda Uluslararası İlişkilerin Değişen Parametreleri, Yüksek Lisans Tezi, Konya: Selçuk Üniversitesi, 2018. s.17.
5. AKYEŞİLMEN, Nezir, Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik, Ankara: Orion Kitapevi, 2018. s.15.
6. ÇELİK, Soner, “Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım”, Academic Review Of Humanities And Social Sciences, Vol:1, Issue:2, 2018. s.3.
7. Fletcher, T. (2011). Twiplomacy – Riding the Digital Tiger. <https://www.gov.uk/government/news/twiplomacy-riding-the-digital-tiger>. pg. 8
8. Melissen, J. (2005). The New Public Diplomacy, Soft Power in International Relations. New York: Palgrave MacMillan. pg. 72