УДК 327.8

КИБЕРДИПЛОМАТИЯ КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

Омарова Динара Куанбековна
omarova.1999@mail.ru
Студентка 3 курса факультета международных отношений
ЕНУ им. Л.Н. Гумилева, Нур-Султан, Казахстан
Научный руководитель – Г.Ж. Кенжалина

По мере того как продолжают развиваться информационно-коммуникационные технологии (ИКТ), развиваются возможности и проблемы, связанные с ними. Мы находимся на перепутье, когда человечество переходит от общества уже переплетенного с Интернетом к будущему веку автоматизации, Big Data (большого количества данных) и InternetofThings (Интернету вещей). Динамичное развитие ИКТ и интернета не знает границ и, как следствие, оказывает трансформирующее влияние на все сферы общества и государства, включая международную политику и дипломатию, в том числе.

Наиболее широкое развитие получила и виртуальная реальность, представляющая собой, создаваемый техническими средствами мир и передаваемая человеку через его привычные для восприятия материального мира ощущения. Здесь вытекает такое понятие, как *киберпространство*. Именно оно является виртуальной реальностью, представляющей ноосферу, второй мир как «внутри» компьютеров, так и «внутри» компьютерных сетей. Киберпространство имеет существенное отличие от наземного, морского, воздушного и космического пространств: оно создано не природой, а является искусственной конструкцией, имеющей компоненты, которые могут меняться с течением времени [1].

В нынешнем мире быстрый подъем разного вида киберугроз создает весьма важной проблему обеспечения информационной безопасности. В свою очередь киберугроза – это противозаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения социальных, политических или иных целей. Киберугрозы способны влиять на информационное пространство компьютера, в котором находятся данные, хранятся материалы физического либо виртуального устройства. В наше время все без исключения киберугрозы принято разделять на внутренние и внешние. Причины и источники внешних угроз находятся вне компьютеров компании, как правило, вовсемирной сети. Внутренние угрозы зависят исключительно от программного обеспечения и оборудования, а также персонала компании. Вирусы, спам, удаленный взлом, фишинг, DoS/DDoS-атаки, хищение мобильных устройств относят к внешним угрозам. Например, вирусы, используя для своих целей трафик, каналы связи, рассылая спам, способны нарушить работоспособность программ и компьютеров, уничтожив данные и файлы. Более опасным вирусом, возникнувшим практически в последнее время, является кибероружие, которое нацелено в некоторых случаях на ликвидацию индустриальной инфраструктуры.В последние несколько лет все более актуальной становится защита от такой внешней угрозы, как хищение мобильных устройств, в памяти которых очень часто хранится в открытом виде важная корпоративная информация: персональные данные клиентов и сотрудников, финансовая документация, электронная переписка, интеллектуальная собственность, а также разного рода пароли и идентификационные данные. Кроме этого, существует еще промышленный шпионаж, кража аппаратного обеспечения, преднамеренное причинение ущерба.

Что касается внутренних угроз, то самую значительную угрозу в наше время представляют уязвимости программного обеспечения. Программы пишутся людьми, а им, как известно, свойственно ошибаться. Недоработки и ошибки в наиболее известных программах позже обнаруживают хакеры, и именно эти ошибки ложатся в основу

большинства вирусов, троянских программ, червей, которые проникают через эти лазейки на компьютеры.

С началом технологического прогресса истории начали создаваться новые возможности, но всегда найдутся и те, кто использует данные возможности для собственной же нужды и прибыли. Несмотря на угрозу вирусов и вредоносных программ, люди были уверенны в том, что их данные в компьютерных системах безопасны и неприкосновенны. Однако это было до тех пор, пока не произошел взрывной рост воздействий машин в Интернете, которые обеспечили настоящую площадку для хакеров, идущих на различные преступления: кражи данных, совершение мошенничества, взлом засекреченных документов, файлов и т.п. Именно это получило название *киберпреступность*. В связи с этим можно выделить такую яркую личность, как Джулиана Пол Ассанжа, австралийского интернет-журналиста и телеведущего, основателя сайта WikiLeaks. Сайт WikiLeaks представляет собой портал, который вот уже более 10 лет наводняет мир сенсационными расследованиями, секретными материалами, взятыми или украденными в спецслужбах передовых стран. Джулиан Ассанж стал культовой фигурой журналистики, в Америке его называют шпионом и предателем, в других странах – человеком, борющимся за свободу слова. В больших объёмах он обнародовал сверхсекретные материалы о шпионских скандалах, коррупции в высших эшелонах власти, военных преступлениях и тайнах дипломатии великих держав. Не раз он находился под арестом и обвинялся в киберпреступлениях. Инцидент с Эдвардом Сноуденом также является показательным фактом того, насколько интернет-коммуникации и взаимозависимость социальной среды с политикой, экономикой и военным сектором стали важны и влияют на стратегическое планирование лидеров ведущих держав мира. Л.В. Савин утверждает, что если в геополитике уже достаточно разработан научный аппарат и дефиниции, которыми оперируют политики, эксперты и ученые, то киберпространство в какой-то мере представляет собой «terraincognita», и за обладание этим пространством ведется довольно активная борьба. Крайне показательным является то противостояние, которое заняли в отношении регулирования интернет-пространства различные государства [1].

Совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями, называют кибербезопасностью. Сегодня основными задачами обеспечения безопасности считаются: доступность, целостность, включающая аутентичность, а также конфиденциальность. Тем самым, кибербезопасность является необходимым условием развития информационного общества, так как кибербезопасность сочетает в себе набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды или киберпространства ресурсов организаций и пользователей. Таким образом, кибербезопасность – это достижение сохранения свойств безопасности, ресурсов организации или пользователей.

В связи с появлением новых технологических разработок начинает развиваться и дипломатия в международных отношениях. Благодаря новым технологиям мир, в котором мы живем сегодня, открывает новые возможности и вызовы для дипломатии. С одной стороны, из-за новых и лучших технологий (например, увеличения количества авиаперевозок, роста интернета, мобильных телефонов, социальных сетей) мы теперь можем общаться друг с другом проще и дешевле, чем когда-либо прежде. Мы можем делиться идеями, решать проблемы и поддерживать этот контакт через социальные сети, используя ИКТ. В то же время существуют и проблемы при работе над международной дипломатией, над обеспечением определенной среды и пространства. Например, интернет, веб-сайты, электронная почта и другие социальные сети, в том числе и СМИ, могут предлагать интересные способы поддержания связи между людьми, странами и т.п. Однако существуют серьезные риски при проведении дипломатии через эти среды. Такие проблемы, как информационная война или кибервойна, представляющая собой бескровную, но в то же

время смертельную войну, киберпреступность с использованием кибероружия, предназначенное для нанесения ущерба в киберпространстве, по-прежнему представляют собой реальную угрозу для защиты информации.

Кибердипломатия может быть определена как дипломатия в киберпространстве или, другими словами, использование дипломатических ресурсов и выполнение дипломатических функций для обеспечения национальных интересов в отношении киберпространства. Такие интересы обычно определяются в национальных стратегиях киберпространства или кибербезопасности, которые часто включают ссылки на дипломатическую повестку дня. Преобладающие проблемы в кибер-дипломатической повестке дня включают кибербезопасность, киберпреступность, укрепление доверия, свободу интернета и интернет-управление.

Кибердипломатия следовательно проводится полностью или частично дипломатами, встречающимися в двусторонних форматах (например, американо-китайским диалогом) или на многосторонних форумах (например, в ООН). Помимо традиционной компетенции дипломатии, дипломаты также взаимодействуют с различными негосударственными субъектами, такими, как руководители интернет-компаний (таких как Facebook или Google), технологических предпринимателей или организаций гражданского общества.

Кибердипломатия - относительно новая концепция. Этот термин использовался раньше, но в основном для описания деятельности «электронной дипломатии». «Электронная дипломатия», которую также называется «цифровой дипломатией» обозначает применение новых технологий и социальных медиа в контексте традиционной деятельности дипломатов, в том числе для консульских целей. По словам Тома Флетчера, электронная дипломатия официально родилась 4 февраля 1994 года, когда тогдашний шведский премьер-министр Карл Бильдт отправил первое дипломатическое электронное письмо президенту США Биллу Клинтону, поздравив его с отменой эмбарго против Вьетнама.

Рассматривая возникновение кибердипломатии, важно сначала понять основную логику сотрудничества в этой области политики. Киберпространство объединяет ряд характеристик, которые обеспечивают дипломатическое взаимодействие между заинтересованными сторонами. Начнем с того, что это глобальный домен, связывающий страны и граждан по всему миру различными способами, порождающими взаимодействия и трения между ними. Кроме того, киберпространство обычно рассматривается как «глобальное общее», определяемое как «ресурсная область, к которой все страны имеют законный доступ». Тогда киберпространство сопоставимо с другими глобальными достояниями, такими как открытое море, воздушное пространство и космическое пространство. По этой причине считается, что требуется минимум правил и положений для обеспечения доступа всем и предотвращения конфликтов, которые могут быть только результатом дипломатических переговоров. Эти принципы международного сообщества сталкиваются со спорным характером киберпространства, в котором его основные державы продвигают конкурирующие видения, интересы и ценности для киберпространства. Другие соответствующие характеристики этой сферы включают в себя:

• сложность атрибуции (подлинности, авторства) кибератак и вторжений, препятствуя доверию между заинтересованными сторонами;

• преимущество правонарушения над обороноспособностью, способствующее агрессивному поведению;

• цифровой разрыв между основными кибер-державами и развивающимися странами, которые создают глобальную уязвимость.

Кроме того, в отличие от других областей международной сферы, государствам сложно полагаться на устрашение путем возмездия, когда дело доходит до киберпространства, из-за проблем с атрибуцией, в частности, несмотря на то, что возможны и другие формы сдерживания. Все эти характеристики делают как международные кибер-отношения, так и управление киберпространством чрезвычайно сложными и хрупкими, но в

то же время делают дипломатию более необходимой, особенно с учетом механизмов укрепления доверия и разработки международных норм и значения.

Таким образом, сотрудничество в киберпространстве - это выбор, а не данность. Например, в обращении к сотрудникам Агентства национальной безопасности в 2015 году Барак Обама упомянул о напряженности с Китаем в качестве примера, когда США могли бы принять конфронтационную позицию «или, альтернативно, (...) попытаться установить некоторые основные правила пути с точки зрения наших действий». В Мировом Порядке Генри Киссинджер дает, пожалуй, самые ясные аргументы, лежащие в основе развития кибердипломатии, подчеркивая, что отсутствие диалога и дипломатии будет пагубно сказываться не только на киберпространстве, но и на более широком мировом порядке:

Путь к мировому порядку может быть долгим и неопределенным, но никакого значимого прогресса нельзя добиться, если один из самых распространенных элементов международной жизни исключается из серьезного диалога. При отсутствии каких-либо формулировок ограничений и согласия по взаимным правилам сдержанности кризисная ситуация может возникнуть, даже непреднамеренно; сама концепция международного порядка может быть подвержена нарастающим напряжениям.

Цель кибердипломатии заключается в постепенном изменении моделей поведения и отношение к пространству мирного сосуществования, определяемое четкими правилами и принципами: от системы интерактивных единиц до общества государств. В этой связи кибердипломатия - это киберпространство, фундаментальная основа международного сообщества, относящаяся к международным отношениям.

Кибердипломатия – политика национальных государств в области обеспечения международной кибербезопасности и сотрудничество по этому вопросу с другими странами.Именно сотрудничество с другими странами в сфере кибербезопасности способно помочь созданию коллективной киберзащиты. На сегодняшний день сотрудничество стран в установлении мира и стабильности международного сообщества, а также национальной безопасности играет большую роль. Кибердипломатия же представляет эволюцию публичной дипломатии для включения и использования новых платформ коммуникации в XXI веке. Как пояснил Ян Мелиссен в своей работе «Новая публичная дипломатия: мягкая сила в международных отношениях», кибердипломатия «связывает влияние инноваций в области коммуникации и информационных технологий на дипломатию» [2]. Кибердипломатия также является частью дипломатии: публичной и виртуальной. Кибердипломатия в качестве основы имеет то, что «она признает, что новые коммуникационные технологии открывают новые возможности для взаимодействия с более широкой общественностью путем принятия сетевого подхода и использования большей части все более многоцентровой глобальной взаимозависимой системы [3]».

Под цифровой дипломатией подразумевается использование современных информационно-коммуникационных технологий для реализации дипломатических и сопряженных внешнеполитических задач. В последние годы значение цифровой дипломатии в международной практике неуклонно растет. Наряду с устоявшимися методами работы внешнеполитических ведомств различных стран и традиционными каналами доведения информации через радио, телевидение и прессу, интернет все шире используется для пропаганды, сбора информации, оказания давления на иностранные правительства, подготовки активистов и стимулирования протестных движений. Основной целью цифровой дипломатии является продвижение внешнеполитических интересов, информационная пропаганда через интернет-телевидение, социальные сети и мобильные телефоны, направленные на массовое сознание общественности и политической элиты [4].

Казахстан, как и любая другая страна, исключительно заимствующая передовые ИКТ, включая технологии обеспечения кибербезопасности, разработанных в других странах, в любой момент может столкнуться с ситуацией, в которой мы выступим в качестве объекта

экспериментов или действительной атаки на критически важные объекты информационно-коммуникационной инфраструктуры страны со стороны преступных организаций и отдельных лиц с непредсказуемым результатом.

Для Казахстана ИКТ играют огромную роль в развитии юного государства.

Область автоматизации государственных услуг, рынок электронной коммерции и электронных платежей развивается на принципах обеспечения безопасности личности, общества и государства при использовании ИКТ, а также воплощения деятельности на базе единых стереотипов, обеспечивающих надежность и маневренность объектов информатизации и связи.

Глава государства Н. Назарбаев в своем Послании народу Казахстана от 31 января 2017 года «Третья модернизация Казахстана: Глобальная конкурентоспособность» отметил, что все большую актуальность приобретает борьба с киберпреступностью. В связи с этим Глава государства поручил Правительству создать систему «Киберщит Казахстана», которая будет обеспечивать защиту электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, систему, способствующую устойчивому развитию Республики Казахстан в условиях глобальной конкуренции [5].

Список использованных источников

1. Л. В. Савин. Кибергеополитика// журнал: «РоднаяЛадога».Москва.2013.С.1-4 http://rodnayaladoga.ru/index.php/natsionalnaya-bezopasnost/382-kibergeopolitika
2. Melissen, Jan. Palgrave Macmillan// «The New Public Diplomacy:Soft Power in International Relations».2007. USA. P. 27-30 http://culturaldiplomacy.org/academy/pdf/research/books/soft_power/The_New_Public_Diplomacy.pdf
3. Melissen, Jan. Palgrave Macmillan// «The New Public Diplomacy:Soft Power in International Relations».2007.USA.P. 56-57 http://culturaldiplomacy.org/academy/pdf/research/books/soft_power/The_New_Public_Diplomacy.pdf
4. А. Крикунов. Центр анализа террористических угроз // «Цифровая дипломатия и ее значение в международной практике».Москва. 2015.С.1-3 https://www.catu.su/analytics/1089-cifrovaja-diplomatija-i-ee-znachenie-v-mezhdunarodnoj-praktike
5. «Послание Президента Республики Казахстан Н.Назарбаева народу Казахстана» // Общественно-политическая газета Казахстана «Время».- 31.01.2017 https://time.kz/news/politics/2017/01/31/poslanie-prezidenta-respubliki-kazahstan-n-nazarbaeva-narodu-kazahstana

УДК 327.1

ОСНОВНЫЕ ПУТИ ОПТИМИЗАЦИИ ПОЛИТИКИ СТРАН ЦЕНТРАЛЬНОЙ АЗИИ В ОБЛАСТИ УСТОЙЧИВОГО РАЗВИТИЯ

Руслан Амина
jumadilova82@mail.ru
Студентка 3 курса факультета международных отношений
ЕНУ им. Л.Н. Гумилева, Нур-Султан, Казахстан
Науный руководитель – А.К. Альпеисов

Центральная Азия - одна из крупнейших макроэкономических зон мира, расположенная в самом центре Евроазиатского субконтинента. Сегодня регион Центральная Азия представляет собой огромную территорию с богатейшими человеческими и