20 лет сотрудничества в рамках программы «Партнерство ради мира»: уроки и перспективы дальнейшего развития потенциала сотрудничества

Алматы - 2015

УДК 327
ББК 66.4
Д22

Сборник издан при финансовой поддержке Департамента публичной дипломатии НАТО

Д 22 20 лет сотрудничества в рамках программы «Партнерство ради мира»: уроки и перспективы дальнейшего развития потенциала сотрудничества. Сборник материалов международной научно-практической конференции. Алматы 9-10 октября. – Алматы, 2015. – 165 с.

ISBN 978-9965-12-408-2

В данном сборнике содержатся статьи, посвященные вопросам новой роли НАТО, итогам Уэльского саммита НАТО, вопросам сотрудничества стран Центральной Азии с НАТО в рамках программы «Партнерство ради мира», перспективы взаимоотношений по вопросам урегулирования ситуации в Афганистане

Данный сборник предназначен для экспертов в области международных отношений и широкого круга читателей, интересующихся вопросами сотрудничества Казахстана и других стран Центральной Азии с НАТО

УДК 327
ББК 66.4

Точка зрения авторов может не совпадать с мнением редколлегии

20 лет сотрудничества в рамках программы «Партнерство ради мира»: уроки и перспективы дальнейшего развития потенциала сотрудничества. Сборник материалов международной научно-практической конференции. Алматы 9-10 октября.

ISBN 978-9965-12-408-2

СОДЕРЖАНИЕ

К.Б. Беков

Кибер безопасность: секьюритизация и противоречия в определении политики безопасности

Безопасность государства как объект изучения долгое время рассматривался преимущественно в военно-политическом аспекте. Однако с окончанием «холодной войны» и снижением угрозы ядерной войны содержание понятия безопасности начало меняться. Данный процесс имел два аспекта. С одной стороны, понятие безопасности начало рассматриваться в расширенном контексте. Так в сферу национальной безопасности начали включаться такие вопросы как экологическая безопасность или информационная и технологическая, транскультурная безопасность и т.п.

С другой стороны расширенное толкование понятия безопасности сопровождалось размытием границ между сферами безопасности. Например, такие явления как терроризм, кибер угрозы, пандемии часто ставят под сомнение релевантность традиционного разделения на безопасность внутреннюю и международную.

Расширение понятия безопасности отобразилось и в разнообразии подходов к изучению данной проблематики. Также стоит отметить, что на данный момент в науке не сложилось четкого определения как внутренней, так и внешней безопасности. Тем не менее, для классических школ по изучению безопасности был характерным подход к рассмотрению безопасности, в качестве некоего объективного состояния которого можно достичь путем проведения тех или иных действий.

Другие исследователи рассматривали категорию безопасности в качестве нормативного понятия, отмечая различия в определении угроз у разных государств в силу особенностей их географического положения, экономической системы, экологического и политического окружения.

Среди различных теоретических подходов к изучению проблем безопасности хотелось бы выделить концепцию секьюритизации развивавшейся в рамках конструктивистских исследований международных отношений. Главной особенностью данной концепции является ее интерпретация безопасности как процесса. [1]

В то время как классические подходы концентрировались в основном на материальных или количественных аспектах безопасности (военный потенциал, соотношение сил, полярность) секьюритизация подразумевает процесс превращения той или иной проблемы в объект политики безопасности.

Это означает, что некий актор интерпретирует какую-либо проблему в качестве вопроса национальной безопасности. Данную интерпретацию актор предлагает адресату и путем его убеждения добивается принятия необходимых актору мер. В процессе секьюритизации актором может выступать правительство, политическая партия, государственное учреждение либо отдельные политики. А в качестве адресата может выступать общественность, парламент либо само правительство. Сам процесс секюритизации может проходить в виде формирования актором у общества (адресата) образа некого объекта или процесса как угрозы. Это в свою очередь приводит к принятию политических мер, например путем принятия законов, выделения средств, создания различных органов или путем кадровых перестановок. Таким образом, процесс секьюритизации угрозы приводит к тому, что некая проблема усилиями тех или иных политических сил приобретает чрезвычайный характер и становится приоритетной по сравнению с остальными вопросами.

Секьюритизация киберпространства является одним из актуальных и наиболее сложных средств в борьбе с возникающими угрозами. Теория секьюритизации, разработанная в рамках Копенгагенской школы, предполагает, что в международных отношениях проблема приобретает характер угрозы и становится объектом неотложной политики посредством провозглашения её таковой влиятельным актором, который тем самым получает легитимизацию общества предпринимаемым чрезвычайным мерам для её устранения.

В качестве одной из отличительных черт киберпространства указывается отсутствие национальных и физических границ. Киберпространство это анархичная структура, в которой, угрозы и ответы на них могут пересекать любые границы и регулирование которой вызывает значительные трудности. Особенностью кибер угроз также является то что, подобная угроза не может быть обнаружена до определенного инцидента, учитывая, что объектом атаки могут стать системы, действующие без прямого и постоянного управления человеком.

Трансграничные угрозы в киберпространстве могут быть направлены на корпорации, общественные организации, отдельные лица и государственные образования, точно также они могут и исходить от корпораций, общественных организаций, частных лиц или государств из любой другой части мира. Кроме того, между любыми из этих единиц могут быть созданы объединения как в пределах одной территории, так и трансграничные – с целью повышения или снижения потенциальной угрозы.

Таким образом, субъекты секьюритизации в сфере кибер безопасности, как правило, являются более крупными референтными

единицами (например, государства, международные организации, транснациональные и национальные корпорации) или более мелкими единицами с представительным статусом при своих более крупных образованиях.

Поскольку киберугрозы являются совершенно новым, ранее неизвестным видом угроз безопасности, потребуется совершенно новый набор ресурсов для борьбы с ним.

Начиная с 2000-х годов в списке угроз в политике безопасности различных стран наряду с терроризмом, сепаратизмом, экологическими вопросами начинают фигурировать и кибер угрозы. Это было связано с несколькими факторами. Во-первых, по мере экономического роста в развитых странах стремительно развивался сектор информационных и коммуникационных технологий.

В современном мире кибер угрозы делятся на три группы: кибер преступность, информационные войны и пропаганда, киберугрозы военного характера. Подобное деление кибер угроз по мнению некоторых специалистов может свидетельствовать об отсутствии в среди политиков и исследователей единого подхода к кибер угрозам. Другим фактором также является неопределенность в вопросе государственного органа который должен был бы нести основную ответственность по обеспечению кибер безопасности. Относительно хакерских атак и кибер преступности в целом в различных обществах существуют разные трактовки об их источнике.

Также интересным является восприятие социальных сетей властями различных стран. Зачастую в прессе и в заявлениях властей социальные сети характеризуются как источники дезинформации, распространения слухов, паники которые могут привести к социальному кризису, хаосу и политической дестабилизации. При этом в общественных дискуссиях также нет единства о внешнем или внутреннем происхождении угроз связанных с социальными сетями. При этом подчеркивается, что усилия властей по контролю над Интернетом вызваны необходимостью защиты суверенитета и единства страны.

В военной сфере представители вооруженных сил неоднократно отмечают растущий процесс об «информатизации» современных войн и в частности о задачах победы в локальных войнах в условиях информатизации. При этом военные в своих выступлениях неоднократно указывали на то, что существующее доминирование США в киберпространстве представляет собой одну из ключевых уязвимостей для безопасности других стран.

Как видно из этих примеров в различных странах при существующем или возможном консенсусе по фундаментальным вопросам кибер безопасности выражающемся в единстве позиций относительно важности

экономической и информационно-пропагандистской функций киберпространства или понимания вооруженными силами значения информационных технологий в военном деле существуют серьезные различия по оценке происхождения, характера и мерам противодействия кибер угрозам.

Тем не менее, на сегодняшний день ведется достаточно успешная политика по донесению до широких масс опасностей которые представляют различные кибер угрозы. Причем это касается не только защиты отдельных граждан от кибер преступности но также и в обеспечении общественной поддержки усилий правительств, корпораций и общественных организаций по установлению контроля над киберпространством.

С другой стороны теория секьюритизации применительно к вопросам кибер безопасности также имеет ряд недостатков. Согласно модели секьюритизации, признание той или иной проблемы проблемой безопасности возможно при условии признании этого со стороны референтной группой. Однако специфика кибер пространства, его новизна и сложность для понимания серьезно затрудняют формирование в обществе единого подхода по политике безопасности в этой сфере.

Существует ряд проблем, относительно секьюритизации которых есть определенные сложности в силу свойственных внутренних противоречий. В данном контексте самый крупный комплекс проблем связан с глобальным характером кибер пространства. Киберпространство является абсолютно новым измерением человеческой деятельности и характеризуется существующей невозможностью ее фрагментации на национальные сектора. Иначе говоря, в цифровом измерении невозможно провести государственную границу и осуществлять национальный суверенитет над ее отдельными частями. Попытки некоторых государств создать защитные барьеры не привели к результатам, которые, можно однозначно трактовать как успешные. [2]. Система фильтрации контента и зарегулированности Интернета в долгосрочной перспективе может иметь негативное влияние на экономическое и научно-техническое развитие страны. Также, фильтрация и регулирование контента вступает в противоречие нормами принципами свободы слова и свободы информации.

С другой стороны, не информационная революция намного опережает темпы реагирования со стороны государства и скорость осознания обществом всего комплекса проблем безопасности связанных с кибер угрозами. Так, в последние годы произошли значительные изменения в сетевых технологиях, а именно широкое распространение мобильного интернета. Этот процесс будет продолжаться и в будущем с развитием

новых технологий беспроводной связи, ростом скорости передачи данных. Весь масштаб распространения беспроводного интернета и его политические последствия еще предстоит оценить в будущем.

Расширение кибер пространства ставит перед государствами ряд трудных дилемм. Например, Интернет наиболее полезен и важен в качества глобальной сети, что требует наличия единых технологий и стандартов касающихся ПО и оборудования. На сегодняшний наибольшие усилия по развитию интернет технологий прилагаются ограниченной группой развитых стран, которые и определяют эти стандарты. Инициативы и попытки отдельных стран по внедрению и разработке альтернативных стандартов при всей перспективности с точки зрения национальной безопасности и суверенитета не имеют будущего, так как в этом случае обесценивается сама идея кибер пространства как единой сети получения, передачи и хранения информации. Именно поэтому попытки таких стран как Россия или Китай по разработке, к примеру, национальных операционных систем не имеют успеха [3, 4]. С другой стороны, применение «сторонних» продуктов и технологий несет в себе потенциальную угрозу безопасности данных и связи.

Другим аспектом кибер безопасности является защита промышленных и стратегических объектов от кибер атак и диверсий. Широкой известный случай с вирусом «Stuxnet» нанесшим значительный урон иранской ядерной программе является наглядным доказательством реальности подобных угроз [5]. В связи с этим, необходима модернизация систем информационной безопасности на предприятиях и коммерческих объектах. При этом, решение данной проблемы требует активного сотрудничества между государством и частным сектором. Это объясняется тем что, борьба против вредоносного программного обеспечения и устройств в силу своей специфичности и сложности бывает зачастую не под силу частным организациям различного профиля.

Растущая информатизация также оказывает значительное влияние на военную сферу. Киберпространство рассматривается как новое поле боя, господство над которым может обеспечить победу в войне. Согласно существующей классификации кибер-атаки имеют множество форм и целей включая вандализм, пропаганду, дезинформацию, разведывательную деятельность, вмешательство в работу или вывод из строя объектов гражданской и военной инфраструктуры и оборудования. С военной точки зрения кибер-атаки представляют достаточно сложную проблему в силу ряда своих специфических черт.

Во-первых, это проблема определения противника. Современные программные средства позволяют проводить масштабные анонимные атаки или же атаки через сети третьих стран. В этом случае страдает

точность и адекватность ответного удара и это может привести к непредсказуемым последствиям. Проблема определения агрессора также усложняется тем что, отдельные группы людей могут организовать подобные атаки по личной инициативе и без санкции своих правительств.

Во-вторых, существуют трудности с определением акта кибер-атаки или агрессии. Нет четкого описания того, какие именно действия могут рассматриваться в качестве акта агрессии при понимании того что, для современного индустриального/постиндустриального общества масштабная кибер-атака может стать фактором поражения в войне.

По мере развития и распространения интернет технологий в различных странах мира актуальность вопросов кибер безопасности будет только возрастать. Это особенно важно для развитых государств т. к. они являются наиболее зависимыми от них. Весь существующий комплекс проблем связанных с кибер безопасностью проблем требует тщательного изучения и последующей разработки мер по укреплению безопасности государства.

Изучение проблем секьюритизация кибер угроз представляет интерес с точки зрения легитимизации чрезвычайных мер со стороны государства по отношению к кибер угрозам, формированию их образа в общественном сознании. Политика по борьбе с кибер угрозами имеет свои особенности, проистекающие из политической культуры, политических институтов, специфики отношений между властью и обществом.

Концепция секьюритизации как инструмент изучения политических процессов в сфере безопасности может быть с успехом использована для изучения проблем безопасности в незападных государствах. Особенности секьюритизации кибер угроз заключаются в том, что на данный момент еще не сформирован единый подход к кибер угрозам как к целостному явлению. Имеются разные мнения относительно основного источника, преимущественного характера и стратегии борьбы с данным явлением.

Цитируемая литература

1. Аветян А. Копенгагенская школа (секьюритизация) // http://avetyan.livejournal.com/21273.html

2. HTG Explains: How the Great Firewall of China Works // http://www.howtogeek.com/ 162092/htg-explains-how-the-great-firewall-of-china-works/

3. Грамматчиков А. Быть ли «русской Windows»? // Эксперт. – 2012. -№8 (791) 27 фев // http://expert.ru/expert/2012/08/byit-li-russkoj-windows/

4. Бевза Д. Китай против всех // http://www.gazeta.ru/tech/2014/08/29_a_6193601.shtml (29.08.2014)

5. Falliere N.s, O Murchu L., Chien E. W32.Stuxnet Dossier. Version 1.4 (February 2011) // http://www.symantec.com/content/en/us/enterprise/media/security_response

СВЕДЕНИЯ ОБ АВТОРАХ

М.А. Абдраимов	Заведующий кафедрой международных отношений Дипломатической Академии МИД Кыргызстана
А.А. Акатаева	Старший преподаватель кафедры международных отношений и мировой экономики КазНУ им. аль-Фараби
Д. Афентули	Координатор программ по Центральной Азии ДПД НАТО
А.Р. Ахметалин	Заместитель начальника Учебного центра «Партнерство во имя мира» Военного института Сухопутных войск
К.И. Байзакова	Директор Ресурсного и информационного центра о НАТО, профессор КазНУ им. аль-Фараби
Г.С. Байкушикова	И.о. доцента кафедры международных отношений и мировой экономики КазНУ им. аль-Фараби
К.Б. Беков	Докторант кафедры международных отношений и мировой экономики КазНУ им. аль-Фараби
М.Б. Бейшенов	Доцент кафедры мировой политики Дипломатической Академии МИД Кыргызстана
А. Винников	Глава офиса НАТО по взаимодействию в Центральной Азии
Г. Глисен	Директор программы изучения Центральной Азии Европейского центра исследования проблем безопасности им. Дж. Маршалла
М.Ш. Губайдуллина	Профессор кафедры международных отношений и мировой экономики КазНУ им. аль-Фараби
Г.Ф. Дубовцев	Главный научный сотрудник КИСИ при Президенте РК
А.Б. Кузембаева	Координатор Ресурсного и информационного центра о НАТО, доцент КазНУ им. аль-Фараби