Секция «Международная безопасность: традиционные вызовы и угрозы»

Концепция «Cross-Domain Deterrence» как внешнеполитический инструмент

Научный руководитель – Веселов Василий Александрович

Голубев Артем Вадимович
Студент (бакалавр)
Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Москва, Россия
E-mail: artyom_golubev99@mail.ru

Бурное развитие технологий в конце XX - начале XXI века привело к появлению новых пространств (или доменов), которые открыли совершенно новые вызовы перед каждым актором на международной арене. Это привело к необходимости их осмысления и создания полноценного ответа. В США для этих целей был создан пост заместителя министра обороны по глобальным стратегическим вопросам (Assistant Secretary of Defense for Global Strategic Affairs), который занял Майкл Нахт. Он организовал проект the 21st Century Cross Domain Deterrence Initiative - встречи ученых, футурологов, целью которого было определить новые угрозы, возникающие от появления новых технологий, так как старая теория сдерживания не давала им нужных ответов. Они определяли термин Cross-Domain Deterrence как использование возможностей одного типа для противодействия угрозам или комбинациям угроз другого типа с целью предотвращения недопустимых атак, т.е. использование технических средств для достижения политических целей[1]. Они пришли к нескольким выводам [2]:

1. сдерживание и противостояния в некоторых пространствах (таких как космос и киберпространство) не может быть ограниченно только ими
2. сдерживание в таких пространствах как космос и киберпространство будет наиболее эффективным при их стигматизации, т.е. создании международных норм, устраивающих всех акторов
3. в такой комплексной среде крайне необходимо понимание восприятия такого рода проблем твоим противником

Хотя термин никогда полноценно не воспринимался правительством США, исследования в этой области были продолжены в рамках инициативы «Минерва», спонсируемая Министерством Обороны США программа по предоставлению грантов для университетских исследований.

Подходящим под новые реалии кейсом, по мнению ученых, стал атака вирусом Stuxnet на объекты иранской ядерной программы. США исчерпали почти все ресурсы для решения этой проблемы ядерной программы Ирана кроме варианта с военным уничтожением объектов, который приводил бы к неизбежной эскалации в регионе. Именно поэтому был выбран вариант с кибератакой. Это привело к тому, что Иран долго не мог определить причины проблем на своих объектах, а при обнаружении вируса - всячески отрицал его сильное влияние на сбои в работе. Аналитики пришли к выводу, что использование кибероружия помогло уравновесить 2 цели: успокоить ключевого союзника и отговорить его от авиаудара по объекту, участвуя в разрушительной, но не кинетической атаке, и как можно дольше не приводить к эскалации, чтобы позволить дипломатическим альтернативам преуспеть в разрешении конфликта[1] [3].

Этот пример наглядно, по моему мнению, идеально показывает, что концепции сдерживания, которые были до этого, не способны дать ответы на такие вопросы как, например: 1) Является ли кибератака актом войны? 2) Как решить проблему одновременно используя свои силовые возможности и не приводя к эскалации ситуации? Во многом, это

было связано с тем, что исследования в области сдерживания ранее были сосредоточены на роли ядерного оружия, при этом мало учитывалось взаимодействие между другими средствами влияния, особенно с киберпространством и космосом.

Несмотря на то, что примеров кросс-доменного сдерживания можно привести достаточное количество еще и до XXI века (например, Карибский кризис 1962 года или Первая война в Персидском заливе 1990-1991 гг.), данной концепции воплощенной в едином документе не существует. Тем не менее, она имеет огромный потенциал для воплощения за счет своей комплексности, которая предоставляет широкий инструментарий возможностей ее применения. Именно поэтому данная концепция и аспекты, связанные с ней, и вызывают значительный исследовательский интерес.

Источники и литература

1) Gartzke E., Lindsay J. “Cross-Domain Deterrence: Strategy in an Era of Complexity”, July 2014 - URL: https://quote.ucsd.edu/deterrence/files/2014/12/EGLindsay_CDDOverview_20140715.pdf - дата обращения: 02.03.2020
2) James A. Lewis, “Cross-Domain Deterrence and Credible Threats,” Center for Strategic and International Studies, July 2010 – URL: https://www.csis.org/analysis/cross-domain-deterrence-and-credible-threats - дата обращения: 02.03.2020
3) Gartzke E., Lindsay J. “Cross-Domain Deterrence: Strategy in an Era of Complexity” – Oxford University Press, 2019 – 384 p.