Цыбаков Д. Л. – докт. полит. наук, доцент
e-mail: d413839@yandex.ru

Развертывание политико-информационных коммуникаций НАТО и Евросоюза в прибалтийском регионе

Приоритетным вектором международных отношений на постсоветском пространстве в XXI столетии стало использование достижений информационной и коммуникационной сфер в целях достижения геополитического доминирования. Наступление эпохи постмодерна во многом определяет особую специфику международно-политической борьбы, где немаловажную роль приобретает практика политической коммуникации. Следует признать правомерность подхода российского исследователя Ф. И. Шаркова, согласно которому политическая коммуникация представляет собой целенаправленную передачу и избирательный прием информационных потоков, что предполагает смысловое взаимодействие политических субъектов во властных отношениях [8, с. 128]. В международном преломлении сущность политических коммуникаций проявляется в трех основных характеристиках: 1) способность информационных потоков беспрепятственно преодолевать национальные границы; 2) возможность массовой коммуникации вносить позитивные или негативные изменения в политические отношения 3) основным субъектом международной коммуникации наряду с национальными правительствами становятся общественные организации и объединения. Однако именно влиятельные государства и мировые державы все еще обладают наибольшей способностью навязывать развивающимся странам алгоритм и режим коммуникации при помощи совершенных технологий и разветвленной инфраструктуры правительственной пропаганды.

Подчеркнем, что эпоха многоплюсного мира представляется невозможной без обмена смыслами между акторами международных отношений. Как обосновывается в научных работах, в XXI столетии коммуникация осуществляются в двух основных проекциях: при помощи открытого влияния и воздействия на контрагентов этого процесса, или же путем скрытого внедрения интересов активного субъекта в смысловое поле и ментальное пространство партнеров по коммуникационному обмену [2, с. 177].

Причем на фоне обострения отношений Россия-Запад политические коммуникации между сторонами все более смещается из диалогового режима в директивный/императивный формат. Первый названный здесь тип коммуникации подразумевает установление доверительных отношений или прагматического партнерства между контрагентами коммуникации, когда все участники данного процесса признают легитимность и суверенность тех, с кем предстоит организовывать информационный обмен.

Для второго из указанных форматов/режимов коммуникации – директивного, согласно авторскому мнению, будет характерным оказание волюнтаристского воздействия на партнера по коммуникации с целью лишения или ослабления его политической субъектности. Такие события, как расширение НАТО на Восток, «олимпийская война» 2008 г. и системный политический кризис на Украине 2014 г. непосредственно сказались на состоянии международных политических коммуникаций между Российской Федерацией и Организацией Североатлантического договора, фактически разрушив контуры диалогового режима информационного взаимодействия «Россия-Запад».

В связи с чем одним из магистральных направлений информационной политики НАТО и действующих в тесной координации с альянсом институтов безопасности

Европейского союза является развертывание в странах прибалтийского региона организационных структур информационного и информационно-психологического противоборства. С помощью созданных во второй половине второго десятилетия XXI столетия Центров НАТО в прибалтийских республиках и Центра Европейского союза в Финляндии атлантические элиты способны реализовывать различные форматы и технологии международной политической коммуникации в геополитическом противостоянии с современной Россией [3, с. 87].

Первым по времени значимым субъектом информационной политики НАТО в ареале Балтии назовем Центр превосходства НАТО по кооперативной кибероборонe, который был открыт в 2008 г. в Таллине, будучи наделен статусом международной военной организации. Центр готовит специалистов для национальных военных структур и других стран НАТО, из 18 млн. евро затрат на создание Центра треть – прямые инвестиции Североатлантического альянса. Размещение указанного подразделения альянса в Таллине отнюдь не случайно – в сравнительно короткие сроки Эстония проделала большой путь к становлению цифрового государства, чему способствовали небольшая территория, численность населения и активная государственная политика в сфере информатизации. В качестве последствия такой политики официального Таллина, отметим, что Эстония, наряду с Литвой, с начала 2000-х гг. традиционно входит в пятерку наиболее развитых государств согласно Индексу кибербезопасности ООН. Так, в 2021 г. прибалтийское государство было размещено экспертами в указанном рейтинге на 3-м месте, тогда как Российская Федерация впервые смогла достичь в нем 5-го показателя. Тремя годами ранее Эстония и Литва помещались на 4-м и 5-м местах в рейтинге кибербезопасности, оставляя Россию только на 28-м месте [14].

Ещё до вступления в НАТО эстонское руководство озаботилось вопросами кибербезопасности. Кроме того, согласно доктрине Североатлантического альянса, кибербезопасность является одной из основных тактических и стратегических задач НАТО. Поэтому, по мнению автора, инициатива по созданию Центра передового опыта НАТО в сфере коллективной кибероборонe принесла большие имиджевые преимущества для внешнеполитического статуса этого не самого влиятельного в современном мире государства. Сегодня 25 стран участвуют в работе Центра, с пятью (Словения, Хорватия, Черногория, Швейцария и Япония) – ведутся переговоры о присоединении, ещё четыре государства (Австралия, Ирландия, Канада и Люксембург) также выразили желание участвовать в информационном взаимодействии [1]. Эстония активно привлекает для решения вопросов кибербезопасности военные, научные, правительственные и бизнес структуры в надежде выстроить междисциплинарный подход для решения проблем киберпространства. Так, созданные в 2018-2019 годах в Эстонии кибервойска и Центр призваны улучшить взаимодействие между всеми видами вооружённых сил и повысить эффективность борьбы с кибертерроризмом [1].

За время своей работы Центр учредил международную конференцию «CyCon», посвященную кибербезопасности. Проводятся ежегодные учения «Locked Shields», где отрабатывается сценарий помощи вымышленной стране в отражении массированных кибератак. Специалисты Центра постоянно прорабатывают сценарии возможных столкновений в киберпространстве, а также цепочку принятия решений на политическом и военном уровнях. С 2010 года проводятся учения «Закрытый Щит», в ходе которых апробируется тактика оказания помощи условному государству в борьбе с внешними кибератаками [4].

Кибер-маневры проходят не только в Таллине, но и удаленно – с участием иностранных команд. В учения «Locked Shields», которые прошли в 2019 г. и стали крупнейшими за всю историю, приняло участие более 1200 человек из 30 стран [1].

В октябре 2018 года руководством НАТО принято решение о создании кибернетических сил, в задачу которых входит нанесение атакующих ударов по противнику в рамках выполнения пятой статьи Устава альянса о коллективной обороне. Кроме того, киберучения НАТО в г. Таллинне «Locked Shields 2019» совпали с открытием Учебного центра по кибербезопасности при Министерстве обороны Эстонии, который готовит специалистов по кибербезопасности и проводит международные учения [1].

В декабре 2019 года под руководством Центра на базе Академии Сил обороны Эстонии прошли масштабные учения НАТО «Cyber Coalition 2019», в которых приняли участие 700 специалистов из 27 стран НАТО и шести партнеров альянса — Японии, Алжира, Австрии, Финляндии, Ирландии, Швеции [13]. В ходе учений разыгрывался приближенный к реальности сценарий киберсражения.

На прошедших в январе 2020 года в Латвии учениях «Cross Sword 2020», курируемых Центром и латышской государственной группой реагирования на киберугрозы «CERT.LT» участники мероприятия из 26-ти стран отработали нейтрализацию системы противовоздушной обороны противника, а также проведение кибератак на его военные и промышленные объекты. Основная цель учений заключалась в добавлении кибердействий в стандартный набор военных инструментов при проведении общевойсковых наступательных операций [3].

В 2020 году в Таллине был опубликован новый справочник по вредоносным программам. Собранные информационные материалы раскрывают значение дизассемблеров[1], средств отладки, методов мониторинга системы и сети, а также методик ликвидации возникающих при коллективной деятельности инцидентов. Основные сведения по функциональным задачам и формам деятельности Центра НАТО в Эстонии представлены в таблице 1.

Таблица 1

Характеристика Центра передового опыта НАТО по кооперативной кибероборонe [13]

Название	**Место расположения**	**Функциональные задачи**	**Формы деятельности**	**Государства-участники**
Центр превосходства НАТО по кооперативной кибероборонe	Таллин, Эстония	- методологическое обеспечение кибер-операций - подготовка кадров - налаживание взаимодействия между членами НАТО информационный обмен с партнерами НАТО	- мониторинг информационных сетей - международные учения - международные конференции - издание пособий по кибер-операциям	23 государства НАТО, Финляндия, Швеция, Украина

Обобщим, что в последние годы НАТО добилось существенных успехов в продвижении директивного формата политических коммуникаций, а Эстония, посредством как развития «киберполигона», так и создания учебного центра вносит заметный вклад в наращивание потенциала проведения кибероперaций в масштабе всего альянса. Российские

[1] Дизассемблер – программное средство, позволяющее преобразовывать машинные коды, объектные файлы или модули в текст программ на удобных для пользователя языках или в текст в закодированных сообщениях.

аналитики указывают на разработку «Таллинского руководства по кибервойне». Не будучи полевым уставом или стратегией информационно-психологического противоборства, фактически он представляет собой обобщенный свод принципов и правил по действиям в пространстве кибер-коммуникаций в ситуации международных конфликтов [4].

Для организации операций информационно-психологического характера предназначен натовский Центр в Латвийской республике. О своем намерении разрешить создание на своей территории «Центра передового опыта НАТО в области стратегических коммуникаций (стратегической пропаганды)» Латвия заявила еще в 2012 году [5, с. 16]. Через два года три прибалтийские республики, а также ФРГ, Италия, Великобритания и Польша на площадке штаба Командования НАТО в США заключили соглашение об открытии международного Центра НАТО, который получил аккредитацию и начал работу в Риге в 2015 г.

Основным направлением деятельности данной структуры является обмен опытом и координация деятельности натовских структур в сфере международных коммуникаций, занимающихся информационными и психологическими операциями, публичной дипломатией и связями с общественностью. Центр НАТО осуществляет подготовку специалистов в области стратегической коммуникации, то есть ведения пропаганды на международном уровне, проводит научно-исследовательские работы по обобщению опыта информационных кампаний, что приводит к выработке новых форм и методов милитаризации международных отношений.

К основным задачам Центра НАТО в Риге относится: определение тематик и форм воздействия на определенную целевую аудиторию; формирование в странах, входящих в зону интересов НАТО, движения радикальной оппозиции из подверженных манипулированию групп населения; проведение PR-кампаний по формированию у целевой аудитории позитивного отношения к политике блока; ограничение информационной политики конкурирующих субъектов международной коммуникации, прежде всего – КНР и Российской Федерации [4].

Особое внимание уделяется следующим направлениям деятельности Центра НАТО в Риге:

– проведение исследований конфликтных ситуаций в информационной среде;

– мониторинг социальных сетей или троллинга, отслеживание кризисных ситуаций на Украине, в Сирии и Ираке, а также изучение деятельности транснациональных террористических группировок;

– выработка методов для штабов НАТО и военных штабов стран-членов, составление плана действий и тренировок военных и гражданских лиц в ситуации информационных конфликтов;

– выработка методов определения и борьбы с лживыми и фейковыми новостями, которые зарождаются в социальных сетях и на интернет-сайтах [6].

Центр НАТО в Латвии тесно сотрудничает с англосаксонскими «фабриками мысли» – Королевским колледжем в г. Лондоне; Стэндфорским университетом. Одним из ареалов активности Центра выступают именно события военно-политического порядка в Балтийском регионе: представительство проводит модерацию и в случае необходимости блокировку публикаций на русском, латышском, литовском и эстонском языках; на платформах, как «Facebook», «Instagram» и «WhatsApp» проводятся кампании по дезинформации, для того, чтоб воздействовать на отдельные государства. Активность работы Центра повышалась в период многонациональных маневров НАТО в Балтийском регионе в период 2017-2020 гг. В

начале 2019 года Центр НАТО договорился о расширении сотрудничества с американской информационной компанией «Facebook», после чего был объявлен конкурс на замещение 150 вакантных должностей [12]. Конкретные функциональные характеристики Центра НАТО в Латвии представлены в таблице 2.

Таблица 2

Характеристика Центра передового опыта НАТО в области стратегических коммуникаций (стратегической пропаганды) [12]

Название	Место расположения	Функциональные задачи	Формы деятельности	Государства-участники
Центр передового опыта НАТО в области стратегических коммуникаций (стратегической пропаганды)	Рига, Латвия	- методологическое обеспечение массовой пропаганды и дезинформации - подготовка кадров - налаживание взаимодействия между членами НАТО - информационный обмен с партнерами организации - продвижение позитивного имиджа альянса - подготовка радикальной оппозиции в постсоветских государствах	- научно-исследовательские разработки -мониторинг информационных потоков и блокировка и сообщений - международные учения - сотрудничество с глобальными интернет-компаниями - проведение пропагандистских акций в СМИ и в сетевом пространстве	Великобритания, Германия, Италия, Канада, Литва, Нидерланды, Польша, Словакия, Франция, Эстония, Финляндия, Швеция

В свою очередь в 2012 г. в столице Литвы создается Центр передового опыта энергетической безопасности НАТО [11].

Несомненной представляется взаимосвязь между развертыванием в Балтийском регионе Центров НАТО и созданием в 2018-2019 годах в системе военной организации Эстонии и Литвы таких формирований как «кибервойска» в формате армейских «батальонов связи». В свою очередь Центры Североатлантического альянса официально призваны улучшить взаимодействие между всеми видами вооружённых сил и повысить эффективность борьбы с кибертерроризмом, что делает их одним из субъектов современной милитаризации.

Именно Национальный центр кибернетической безопасности (НЦКБ) Литвы регулярно проводит учения «Кибернетический щит», к которым привлекаются и предприятия частного информационного сектора, научных учреждений, а также масс-медиа прибалтийских государств. Начиная с июля 2020 г., в литовском Каунасе при поддержке США строится Центр кибербезопасности, на который выделено 1,3 млн долларов. Он предназначен функционировать как подразделение литовского Национального центра кибербезопасности, привлекаясь для управления силами быстрого киберреагирования «единой Европы» [9]. Обобщающие сведения о деятельности Центра НАТО в Литве приведены в таблице 3.

Таблица 3

Характеристика Центра передового опыта НАТО по энергетической безопасности [11]

Название	Место расположения	Функциональные задачи	Формы деятельности	Государства-участники
Центр	Вильнюс,	- выявление угроз в	- научно-	Великобритания,

превосходства энергетической безопасности НАТО.	Литва	сфере международной энергетики - обеспечение защищенности энергетической инфраструктуры - методология помощи в чрезвычайных ситуациях; - рекомендации о развитии альтернативной энергии в сфере военной политики.	исследовательские разработки - курсы и семинары по обеспечению энергобезопасности - международные конференции - международные учения - пропагандистские акции против «Северного потока» и атомной энергетики Белоруссии	Германия, Италия, Латвия, Литва, США, Турция, Франция, Эстония, Грузия, Финляндия

Показательно, что так называемые «кибервойска» в последние годы создаются формально не под эгидой НАТО, а при решающем участии Европейского союза. В январе-марте 2020 года было провозглашено создание Кибернетических сил Евросоюза быстрого реагирования, общая координация которых была возложена на Литву [10]. Именно Литва, начиная с 2017 г. настаивала на объединении усилий членов ЕС в информационной борьбе. Кроме этого государства, в объединенных киберсилах по линии национальных министерств обороны участвуют Эстония, Голландия и представители т.н. «новой Европы» – Румыния, Хорватия и Польская республика. Статус наблюдателя в структуре киберсил получили Бельгия, Греция, Испания, Италия, Франция, Словения и Финляндия. Характерно, что основным объектом противостояния для прибалтийских военных называются не только Российская Федерация, но и КНР [9].

По натовским стандартам в последние годы формируется и структура политико-информационных коммуникаций Европейского союза в Балтийском регионе. В Хельсинки (Финляндия) с 2017 г. работает «Европейский центр передового опыта (практик) по противодействию гибридным угрозам». В рамках указанной структуры происходит взаимодействие между экспертами НАТО и ЕС по противодействию т.н. «гибридным атакам» со стороны России, КНР и других субъектов. При этом под «гибридными угрозами» подразумевались распространение недостоверной информации, посягательство на информационные системы, а также другие виды использования передовых коммуникационных технологий. В работу центра за прошедшие годы вовлечено восемнадцать стран, включая прибалтийские республики, Финляндию, ее скандинавских соседей, а также США, Франция, Германия, Великобритания, Испания и Польша. Будучи наделен задачей составления экспертных оценок по ключевым проблемам безопасности, он в первую очередь занят популяризацией темы так называемой «энергетической войны» России против Запада и Украины, включая дискредитацию прокладки стратегического трубопровода «Северный поток-2» через Балтийское море [5, с. 20]. Особое значение придается концентрация внимания Центра на реалиях Балтийского региона и Севера Европы. Несмотря на немногочисленность сотрудников, в структуре Центра оформлено четыре рабочих группы – «Гибридного влияния» (руководство Великобритании), оценки «Негосударственных субъектов» (Швеция), группа по «Уязвимостям и устойчивости» (Финляндия), группа «Стратегии и обороны» (Германия) [5, с. 19]. Систематизированный материал по функциональным задачам и формам деятельности Центра в Хельсинки представлен в таблице 4.

Таблица 4

Характеристика «Европейского центра передового опыта (практик) по противодействию гибридным угрозам»

Название	Место расположения	Функциональные задачи	Формы деятельности	Государства-участники
Европейский центр передового опыта (практик) по противодействию гибридным угрозам	Хельсинки, Финляндия	- методологическое обеспечение массовой пропаганды и дезинформации - подготовка кадров - налаживание взаимодействия между членами и ЕС и НАТО в сфере международной пропаганды - сотрудничество с международными экспертами и неправительственными организациями	- научно-исследовательские разработки - курсы и семинары по противодействию «гибридным угрозам» - международные тренинги и консультации - пропаганда и контрпропаганда в СМИ и социальных сетях	24 государства ЕС, Великобритания, Канада, Норвегия, США, Черногория

Отметим, что приспособление технологий политических коммуникаций к задачам масштабного информационно-психологического давления на Россию, продекларированное в официальных документах ЕС, коррелируется с предшествующими по времени изменениями в доктринах политических коммуникаций США и НАТО [7, с. 10-11]. После принятия резолюции «Стратегические коммуникации ЕС как противодействие пропаганде третьих сторон» по стандартам атлантического блока вводится в оборот терминология, маскирующая начало открытого пропагандистского воздействия в сфере политической коммуникации СНГ. Заключим, что деятельность центров НАТО способствует милитаризации системы международных коммуникаций на балтийских рубежах современной России, способствуя эскалации отношений «Запад-Российская Федерация», формируя вызовы и риски для национальной безопасности нашей страны.

Литература:

1. Андреев С. Прибалтийский киберфронт НАТО [Электр. ресурс]. URL: https://russiancouncil.ru/analytics-and-comments/analytics/pribaltiyskiy-kiberfront-nato/ (дата обращения: 11.07.2021.)

2. Белозёров В. К. Международная политическая коммуникация в условиях цифровизации мирового развития // Контуры глобальных трансформаций: политика, экономика, право. 2020. Т. 13. № 2. – С. 177-194.

3. Годованюк К. Кибербезопасность и борьба с ней : опыт Великобритании // Научно-аналитический вестник ИЕ РАН. 2019. № 4. – С. 87-92.

4. Савин Л. Центры превосходства НАТО в Прибалтике [Электр. ресурс]. URL: https://www.geopolitica.ru/article/centry-prevoshodstva-nato-v-pribaltike (дата обращения: 12.05.2021).

5. Свиридов А. Европейский центр передового опыта по противодействию гибридным угрозам (2021) // Зарубежное военное обозрение. 2021. № 7. – С. 17-21.

6. Хагельштам А., Наринен К. Противодействие гибридным угрозам НАТО и ЕС [Электр. ресурс] // Вестник НАТО. URL: https://www.nato.int/docu/review/2018/Also-in-2018/cooperating-to-counter-hybrid-threats/EN/index.htm (дата обращения: 12.05.2021.)

7. Глобальная стратегия безопасности ЕС 2016. Аналитический доклад / под ред. Н. К. Арбатовой, А. М. Кокеева. – М.: ИМЭМО РАН, 2017. – 33 с.

8. Шарков Ф. И. Управление политическими коммуникациями путем сегментации политического рынка и позиционирования политических субъектов // Коммуникология. 2014. Т. 5. № 3. – С. 119-128.

9. Литва и США строят инфраструктуру для кибернетической войны [Электр. ресурс]. URL: https://eadaily.com/ru/news/2019/07/03/litva-i-ssha-stroyat-v-kaunase-infrastrukturu-dlya-kiberneticheskoy-voyny (дата обращения: 11.07.2021.)

10. Шесть стран создали Кибернетические силы Евросоюза [Электр. ресурс]. URL: https://www.interfax.ru/world/697858 (дата обращения: 11.07.2021.)

11. NATO energy security Center of Excellence [Электр. ресурс]. URL: https://www.enseccoe.org/en. (дата обращения: 11.07.2021.)

12. StratCom/ NATO Strategic Communications Centre of excellence [Электр. ресурс]. URL: https://stratcomcoe.org/ (дата обращения: 27.07.2021).

13. NATO Cooperative Cyber Defence (CCD) [Электр. ресурс]. URL: https://www.ccdcoe.org// (дата обращения: 21.08.2021).

14. Глобальный индекс кибербезопасности Global Cybersecurity Index (GCI) [Электр. ресурс]. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%... B8_Global_Cybersecurity_Index_(GCI) (дата обращения: 21.08.2021).