**Подводные коммуникационные сети как фактор геополитической борьбы**

***Курочкин Александр Владимирович***

студент 2 курса магистратуры

Московский Государственный Институт Международных Отношений Министерства иностранных дел Российской Федерации, факультет управления и политики, г. Москва, Россия

*jiroki@yandex.ru*

Подводная коммуникационная инфраструктура является одной из важнейших геополитических сфер противостояния в XXI веке. В течение последних 10 лет крупнейшие мировые акторы, включая Соединенные Штаты Америки, Китай, Францию и Россию, а также технологических гигантов, уделяют все большее внимание стратегическому значению кабелей, лежащих на дне океанов. На вопросы безопасности подводных коммуникаций с научной точки зрения впервые обратили внимание Sechrist (2012) [6], Ross (2014) [5] и Martinage (2015) [4]. Научно-практическая значимость работы обусловлена тем, что исследований на тему подводных интернет-коммуникаций в России крайне мало, хотя важность ее бесспорна: международная экономика на 99% функционирует посредством разветвленной оптоволоконной сети. [1] Ежедневные финансовые транзакции на сумму более $10 трлн, потоковое видео, телефонные звонки, дипломатическая и военная почта передаются с помощью 529 подводных кабелей и 1444 наземных станций. [2] Многие государства, банки и рынки завязаны всего лишь на несколько кабелей, разрыв которых может полностью выключить их на несколько недель, что приведет к колоссальным финансовым потерям.

Прокладка подводных кабелей находится в области частного права. Такими проектами обычно занимаются консорциумы, состоящие из крупных телекоммуникационных компаний из различных стран. В настоящее время SubCom из США, Alcatel Submarine Network из Франции, NEC из Японии и HMN Tech из Китая являются четырьмя крупнейшими игроками в этой сфере. Так как эти проекты не аффилированы с определенными государствами, то они и не подпадают под юрисдикцию Конвенции ООН по морскому праву 1982 г. Эдвард Сноуден в 2013 г. раскрыл информацию о том, что государства руками частных компаний полностью контролируют эти коммуникации и не спешат распространить на эту сферу правовые основания, так как подводные кабели используются для сбора информации и шпионажа. [1]

Существуют как естественные угрозы для этой инфраструктуры (от корабельных якорей до землетрясений), так и угрозы диверсии. Эти виды угроз друг от друга практически неотличимы, что является значительным вызовом в области безопасности. При попытке ремонта этих коммуникаций возникает сразу несколько проблем: 1) небольшое количество специализированных судов для обслуживания кабелей (в мире их около 50), 2) расстояния, которые им требуется преодолеть для осуществления ремонтных работ, и 3) значительная глубина залегания инфраструктуры. Уязвимость для диверсий заключается в следующем: 1) расположение кабелей широко известно, 2) концентрация расположения кабелей в узких местах очень высока ввиду того, что не во всех местах океаническое дно удобно для прокладки кабелей (то есть можно повредить сразу несколько кабелей за один раз).

В условиях глобального противостояния военные службы государств могут вести диверсионную работу по разрушению этих коммуникаций. Во-первых, кабели могут быть перерезаны; во-вторых, существует возможность использования беспилотных подводных дронов на дистанционном управлении, оснащенных гидролокаторами высокого разрешения (UUV[[1]](#footnote-1)); в-третьих, наземные станции, принимающие сигнал, также могут стать потенциальной целью; наконец, акторы способны доминировать и без силового вмешательства: посредством строительства этой инфраструктуры, либо обслуживая ее.

Выделяется четыре субрегиона с максимальной концентрацией подводных кабелей: Северная Атлантика, Южная Атлантика, Африка и Индо-Тихоокеанский регион с эпицентром в районе Малаккского пролива. В Северной Атлантике структура подводных кабелей, соединяющих США и Европу, максимально плотная. Южная Атлантика из-за более разреженной структуры подвержена риску внедрения внерегиональных игроков. Африканский континент опоясан плотным кольцом подводных кабелей, идущих как из Европы, так и из Азии. Индо-Тихоокеанский регион характеризуется очень сложной сетью, соединяющей самые густонаселенные и быстроразвивающиеся экономики мира. Именно поэтому он является эпицентром борьбы между Китаем и США за подводные коммуникации. Регион Красного моря и Персидского залива также является зоной повышенного риска, так как в последнее время активизировалось гибридное противостояние между Израилем и прокси-группами, подконтрольными Ирану. [3]

США через свои крупные технологические компании ведут стратегическую борьбу за контроль над подводной кабельной сетью. Китай следует аналогичной модели в регионах мира, где он обладает наибольшим влиянием. Доля Китая в мировом секторе подводных кабелей выросла до 11,4% в 2019 г., при этом Китай стремится увеличить свою долю до 20% в период с 2025 по 2030 г. Расширение влияния в подводных коммуникациях является частью программы «Цифровой Шелковый путь». Франция посредством компании Alcatel Submarine Networks, лидирующей на рынке (доля составляет более 33%), распространяет свою технологическую мощь на Африканский континент. Россия может осуществить угрозу уничтожения ключевых подводных коммуникаций в случае войны с НАТО. Основную часть дебатов по поводу безопасности подводных кабелей вызвала активность подводных лодок России в территориальных водах Европы в 2015 г. Появились опасения того, что Россия может подключиться к коммуникациям, либо перерезать их в рамках «гибридной войны». Также дискуссии об угрозе со стороны России активизировались после начала Специальной военной операции в 2022 г.

Данное исследование показывает, что подводные коммуникационные кабели являются ключевой сферой глобального противостояния в XXI веке. Так как этот аспект находится вне юрисдикции морского права, то государственные и негосударственные акторы могут использовать эту сеть в своих целях без серьезных последствий для себя. Соединенные Штаты Америки продолжают транслировать свою гегемонию руками транснациональных компаний. Китай, в свою очередь, стремится захватить часть рынка, чтобы в рамках «Цифрового Шелкового пути» распространить свое влияние через торговлю и импорт энергоносителей. Франция использует лидера рынка для восстановления своего влияния в Африке. Россия может разрушить ключевые узлы подводных коммуникационный кабелей в случае полномасштабной войны с НАТО. Активизация противостояния между Израилем и шиитскими прокси-группами несет значительный риск для коммуникаций на Ближнем Востоке.

**Литература**

Aldrich R. J., Karatzogianni A. Postdigital war beneath the sea? The Stack’s underwater cable insecurity //Digital War. – 2020. – Т. 1. – №. 1. – С. 29-35.

Cannon B. J., Bhatt P. The Quad and Submarine Cable Protection in the Indo-Pacific: Policy Recommendations. – 2024.

Kurochkin A., Lodina A. & Pankov G. Hybrid Warfare in the Middle East. // Управление и политика. – 2022. – – №. 1 (3). – С. 0–0.

Martinage R. Under the sea: The vulnerability of the commons //Foreign Aff. – 2015. – Т. 94. – С. 117.

1. Ross M. Understanding interconnectivity of the global undersea cable communications infrastructure and its implications for international cyber security //The SAIS Review of International Affairs. – 2014. – Т. 34. – №. 1. – С. 141-155.
2. Sechrist M. New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems. – Harvard Kennedy School, Belfer Center for Science and International Affairs, 2012.
1. Unmanned underwater vehicles (англ.) – беспилотные подводные аппараты [↑](#footnote-ref-1)