Секция «Международная безопасность: новые и традиционные вызовы и угрозы»

Милитаризация киберпространства как новая угроза стратегической стабильности

Чирко Алиса Александровна
Выпускник (магистр)
Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Кафедра международной безопасности, Москва, Россия
E-mail: alessa548@yandex.ru

С развитием новых технологий неизбежно модернизируются средства и форматы коммуникаций как в гражданской, так и в военной сфере. Бурное развитие IT-индустрии открыло для человечества уже пятое по счёту измерение - киберпространство. Являясь полноценной средой взаимодействия государств и других акторов, киберпространство одновременно имеет ряд отличий от иных сред: искусственное происхождение, нематериальный характер субъектов, моментальная скорость распространения информации, отсутствие географических, физических и политических границ [6].

Нынешний конфликт между Россией и Украиной актуализировал множество открытых проблем современной международной безопасности, в том числе, проблему милитаризации киберпространства. Только за 2022 год число кибератак на объекты российской критической информационной инфраструктуры (КИИ) возросло более чем на 80% [2]. Установлено, что большинство из них осуществлялись с территорий стран НАТО, ЕС и Украины.

В 2014 году лидеры стран НАТО подтвердили, что кибератака может являться основанием для применения пятой статьи Североатлантического договора. В июне 2018 года государства-члены Альянса утвердили «Видение и стратегию относительно кибернетического пространства как сферы операций». На саммите НАТО 2021 года в Брюсселе была одобрена «Комплексная политика киберзащиты». Было в очередной раз признано, что кибератаки при определенных обстоятельствах могут рассматриваться как вооруженное нападение [8].

Ещё в 2009 году в США было создано Киберкомандование (United States Cyber Command). Изначально ведомство отвечало за оборону военной информационно-технологической инфраструктуры, однако в 2017 году президент Дональд Трамп выделил этот орган из состава Стратегического командования в отдельное самостоятельное боевое подразделение. Так в военной стратегии США официально появилось направление, отвечающее за формирование наступательного киберпотенциала. В Великобритании подобное подразделение было создано в 2013 году [3].

Боевое применение информационно-коммуникационных технологий (ИКТ) можно условно разделить на техническое воздействие на объекты критической инфраструктуры противника (кибератаки, средства РЭБ) и информационно-психологические операции, направленные как на комбатантов, так и на гражданское население вражеского государства. Ведущая роль операциям в киберпространстве отводится в американской концепции мультидоменной войны, которая предполагает одновременное ведение боевых действий во всех пяти средах [7]. Потенциальными целями ИКТ-атак могут стать компоненты российских Сил ядерного сдерживания (СЯС), что создаёт прямую угрозу для стратегической

стабильности [1]. При этом самые опасные последствия может вызвать атака на системы управления ядерными силами, а также системы предупреждения о ракетном нападении (СПРН) и противоракетной обороны (ПРО) [4].

В 2020 г. Президент России Владимир Путин утвердил «Основы государственной политики в области ядерного сдерживания», где прописаны действия вероятного противника, способные привести к применению ядерного оружия со стороны Москвы [5]. Документ вызвал широкую дискуссию в экспертной среде, особенно пункт «воздействие противника на критически важные государственные и военные объекты РФ, вывод из строя которых приведет к срыву ответных действий ядерных сил». По мнению специалистов, такая трактовка подразумевает в том числе мощную кибератаку на информационную инфраструктуру РВСН с целью выведения её из строя.

До настоящего времени, РФ выступала против применения ИКТ в военно-политических целях и являлась главным инициатором переговорного процесса по формированию норм международно-правового регулирования поведения государств в киберпространстве в рамках ООН. Тем не менее, отсутствие такого регулирования и его ближайшей перспективы сегодня является одним из основных факторов, дестабилизирующих систему международной безопасности.

В связи с этим, Москве целесообразно рассмотреть возможность создания военного киберпотенциала, достаточного для отражения текущих угроз и формирования политики сдерживания в ИКТ-сфере.

Источники и литература

1) Кокошин А.А. Вопросы прикладной теории войны / А.А. Кокошин; НИУ «Высшая школа экономики»». – М.: Изд. Дом Высшей школы экономики, 2018.
2) Коротков С. "О влиянии киберстабильности на обеспечение международной и национальной информационной безопасности" // Журнал "Международная жизнь" URL: https://interaffairs.ru/news/show/38896 (дата обращения: 14.02.2023).
3) Крутских А.В., Бирюков А.В., Бойко С.М., Волкова С.Г., Зиновьева Е.С., Матюхин Д.В., Смирнов А.И. Международная информационная безопасность. Теория и практика. Том 1. - 2-е изд. - М.: "Аспект Пресс", 2021. - 384 с.
4) Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии. - М.: ИМЭМО РАН, 2020. - 98 с.
5) Указ Президента РФ "Об Основах государственной политики Российской Федерации в области ядерного сдерживания" // Сайт Президента РФ URL: http://publication.pravo.gov.ru/Document/View/0001202006020040 (дата обращения: 14.02.2023).
6) Choucri N. Cyberpolitics in International Relations. Cambridge: The MIT Press, 2012.
7) Multi-Domain Battle: Evolution of Combined Arms for the 21st Century, 2025-2040 // TRADOC Headquarters Library. October 2017. URL: https://admin.govexec.com/media/20171003_-_working_draft_-_concept_document_for_multi-domain_battle_1_0.pdf
8) NATO. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm