Секция «Конфликты в цифровом пространстве в условиях становления новых медиакорпораций»

Практика и перспективы государственно-частного партнерства в области кибербезопасности

Научный руководитель – Константинова Елена Анатольевна

Жбанов Артем Михайлович

Аспирант

Московский государственный университет имени М.В.Ломоносова, Факультет политологии, Кафедра международных отношений и интеграционных процессов, Москва, Россия

E-mail: Norvejsky@gmail.com

Роль информационных технологий в современном противостоянии государств и принципиальное смещение противостояния в информационное поле и киберпространство позволяет рассуждать о значительном влиянии информационных технологий на стратегическое планирование мировых держав в области возможных будущих и нынешних конфликтов. Возможность управления политическими конфликтами за рубежом с помощью новых медиа, извлечение выгодных тактических и стратегических преимуществ благодаря информационно-коммуникационным системам по сбору данных, обладание технологиями для вмешательства в работу критически-значимой и стратегической инфраструктуры становятся ключевыми вопросами в области военной составляющей международных отношений. Как отмечает отечественный исследователь Д.Тренин: «Фактически впервые со времен появления ядерного оружия в 1940-х гг. появилась принципиально новая сфера применения силы в международных отношениях»[1].

При этом стоит отметить, что реализация конкурентоспособных технологических решений и инструментария для ведения операций в киберпространстве и защиты от подобных операций тесно связаны с частным сектором и коммерческими структурами, предоставляющими решения в области информационных технологий. Однако вопросы и проблемы взаимоотношений государства и цифровых монополий представляют широкий интерес для исследователей. Характер поведения цифровых транснациональных корпораций в рамках международных процессов, как и их формат взаимоотношений с национальным правительством и регуляторами принципиально отличается от устоявшейся модели деятельности транснациональных компаний как участников международной политики. Данная особенность в экспертно-научном сообществе была отмечена Д.Трениным [2], С.В.Володенковым [3], В.Цзяньганем [4]. Цифровые гиганты становятся агрегаторами огромных массивов данных о пользователях своих виртуальных продуктов по всему миру, что неизбежно создает интерес к ним со стороны государства, на территории которых находятся их инфраструктура и головные офисы. Они становятся проводниками государственной политики и собирают данные для специальных служб, внутри них создаются специализированные проектные группы и подразделения, задействованные в проектах, связанных с чувствительными вопросами национальной безопасности. Ряд журналистов-расследователей отмечает, что ЦРУ инкорпорирует [5, 6] отдельные подразделения технологических корпораций, таких как Meta (признана в России экстремистской организацией и запрещена [7]), а также рекрутирует сотрудников из интересующих направлений в структуру ЦРУ. Также, на этапе финансирования деятельности, согласно утверждениям журналистов, будущий технологический гигант Meta был профинансирован аффилированным с ЦРУ венчурным фондом Accel Partners [8].

Взаимодействие государственного и частного секторов в области обеспечения безопасности широко распространено в США. Преимущественной формой взаимодействия является государственный заказ на конкретную военно-техническую продукцию, проведение научно-исследовательских и опытно-конструкторских работ. Практика создания социальных сетей и инструментов в телекоммуникационной сети Интернет формирует новые условия взаимодействия государства и технологических корпораций и разграничение их компетенций и ответственности на основе взаимной выгоды. На условиях обоюдного согласия коммерческая выгода и функционал в подобных проектах поддерживается частной организацией, а возможности, связанные со сбором информации о пользователях, организацией информационных и политических кампаний как на родине так и за рубежом находятся в ведении специальных служб, обеспечивающих национальную безопасность.

Представляется целесообразным анализ и проработка нормативно-правовой базы для развития российского сектора цифровых продуктов с государственным участием, ориентированного на международные рынки для конкурентоспособности российского разведывательного и политического потенциала.

Источники и литература

1) РСМД: https://russiancouncil.ru/analytics-and-comments/analytics/traditsionnye-i-novye-vyzovy-bezopasnosti-v-mezhdunarodnykh-/.
2) РСМД: https://russiancouncil.ru/analytics-and-comments/analytics/traditsionnye-i-novye-vyzovy-bezopasnosti-v-mezhdunarodnykh-/.
3) Володенков С. Глобальные гибридные акторы информационного вмешательства в современные политические процессы // Политическая экспертиза: ПОЛИТЭКС. 2019. Т. 16
4) Цзяньгань В. Влияние IT-гигантов на политику// Медицина. Социология. Философия. Прикладные исследования. 2019.
5) MintPress News :https://www.mintpressnews.com/about-mint-press-news/.
6) New York Post: https://nypost.com/2022/12/22/facebook-twitter-stocked-with-ex-fbi-cia-officials/.
7) Официальный сайт Генеральной прокуратуры Российской Федерации: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=72267200.
8) The New Zealand Herald: https://www.globalresearch.ca/facebook-the-cia-conspiracy/12685.