Секция «Конфликты в «цифровом обществе»: природа, специфика, механизмы решения»

Политическое измерение киберконфликта

Научный руководитель – Анастасов Александр Иванович

Романов Владислав Витальевич
Студент (магистр)
Донецкий национальный университет, Исторический факультет, Кафедра политологии и государственного управления, Донецк, Украина
E-mail: Jin.Romanov@yandex.ru

В начале XXI века внимание мировой общественности, правительств многих государств приковано к вопросу конфликтов в киберпространстве. Ввиду их нарастающей интенсивности лидеры ведущих промышленно развитых стран с высокоразвитой инфраструктурой информационно-коммуникационных технологий выражают обеспокоенность, так как именно эти страны являются главной мишенью киберпреступников. Целью атак может быть как рассекречивание ядерных объектов, так и военных и/или секретных сетей, а также случайных компьютеров. В результате данной активности формируются целые киберпреступные сети. Зачастую атаки вызваны по причине социальной активности частных лиц с целью кражи интеллектуальной собственности, получения прибыли, либо политических притязаний отдельных государств с целью вмешательства во внутренние дела другого государства.

Обусловленность кибератак в том числе причинами политического (геополитического) характера позволяет нам представить киберконфликт как один из видов политического конфликта. Государства, как один из субъектов киберконфликта, используют киберсредства в качестве способа воздействия на политику другого государства в своих национальных интересах. Политика давления и принуждения посредством кибероперациий имеет несколько характерных особенностей: во-первых, последствия данной преступной активности являются обратимыми, во-вторых, определение виновной стороны является труднодостижимой задачей, так как зачастую государства используют в своих целях частных лиц, которые не несут ответственность перед международными законами и договорами. Одним из доказательств причастности государства к проведённой кибератаке является её структурная сложность.

Немецкий политолог Томас Рид утверждает, что все политически мотивированные кибератаки являются просто изощренными версиями саботажа, шпионажа и подрывной деятельности [3]. Однако киберконфликт не носит насильственного характера, поэтому является способом достижения политических целей без войны между государствами в классическом понимании.

Примерами использования кибератак как инструмента давления в политике является спонсируемая китайским правительством атака на Национальную ассоциацию промышленников США летом 2019 года. Это произошло накануне следующего этапа переговоров между США и Китаем, посвященных возможной торговой сделке. Хакеров интересовали данные, связанные со встречей президента США и руководителя ассоциации промышленников [1]. Таким образом Китай пытался получить преимущество в торговой войне. Ещё одним примером является киберкампания под кодовым названием «Олимпийские игры», проведённая в 2010 году. Вирус Stuxnet был частью киберкампании, проводимой США для нарушения работы систем управления на иранских ядерных объектах. Данная операция была предпринята с целью сдерживания иранской ядерной программы, против которой выступают США. На данный момент президент США Дональд Трамп одобрил проведение кибератаки против Ирана, в результате которой иранские компьютерные системы,

используемые для управления запуском ракет, были отключены [4].

Составной частью киберконфликта являются информационные операции, представляющие угрозу для общества и государственной безопасности. Часть информации, поступающей в киберпространство, заранее сфабрикована и используется в целях манипулирования общественным мнением, что помогает враждебным государствам достичь определенных целей. Авторы докладов ежегодной конференции по киберконфликтам «CyCon 2018» поднимали проблему использования социальных сетей в спонсируемых государствами информационных операциях. С помощью подобных действий государства могут дестабилизировать ситуацию внутри общества целевого государства, навязать своё видение происходящих событий. Широкое распространение дезинформации представляет угрозу национальной безопасности государства, так как способно изменить политические установки граждан. Примером являются протесты в Гонконге. Согласно заявлению руководства социальной сети «Twitter» китайское правительство проводило скоординированную информационную кампанию, направленную на подрыв легитимности гонконгских протестов. В сообщениях, опубликованных связанными с Китаем аккаунтами, утверждалось, что участники протестов в Гонконге извлекают из них «выгоду с помощью плохих ребят» и что у них были «скрытые мотивы» [2]. С помощью этой информационной кампании руководство Китая пыталось урегулировать антикитайские протестные акции, проходившие в автономном Гонконге.

Международное сообщество на данный момент не выработало приемлемый механизм решения киберконфиктов, а также способы регулирования действий государств в киберпространстве. Кибератаки и информационные операции несомненно являются инструментом политического давления, как и бездоказательные обвинения в кибератаках.

Таким образом, киберконфликты выходят за пределы киберпространства и встраиваются в более широкий контекст политических конфликтов. Интенсификация киберконфликтов акцентирует внимание на потенциальных угрозах государственной безопасности, связанных как с атакой на объекты критической инфраструктуры, финансового сектора государств, так и на установки отдельных граждан. На данном этапе необходима грамотная оценка реальных политических последствий киберконфликтов с целью нахождения механизмов их урегулирования.

Источники и литература

1) ТАСС: https://tass.ru/ekonomika/7109613
2) Meduza: https://meduza.io/feature/2019/08/21/kitay-skopiroval-tehnologii-rossiyskoy-fabriki-trolley-i-vpervye-nachal-kampaniyu-po-dezinformatsii-v-tvittere-i-feysbuke
3) ResearchGate: https://www.researchgate.net/publication/233185239_Cyber_War_Will_Not_Take_Place
4) RT: https://russian.rt.com/world/news/643614-tramp-kiberataka-iran