Секция «Политические конфликты в современном мире»

Невидимая вражда: стратегии держав в ведении кибервойны.

Научный руководитель – Лихачева Анастасия Борисовна

Устьянцева Екатерина Александровна
Студент (бакалавр)
Национальный исследовательский университет «Высшая школа экономики», Факультет мировой экономики и мировой политики, Москва, Россия
E-mail: kkate_74@mail.ru

Начало XXI века характеризуется развитием информационных технологий и активным применением их не только в повседневной жизни, но и в политической игре государств. Кибервойны называют войнами будущего, а каждая война подразумевает под собой применение определенного типа оружия и формирование характерной для нее тактики ведения боевых действий.[2] Применение правильной стратегии и своевременное реагирование на вызовы противника во многом определяют место и роль государства на политической арене.[1] Теоретическая и практическая разработка данной области военной науки является актуальной, а ее востребованность в ближайшее время будет лишь возрастать.

Целью данной работы является рассмотрение коммуникативных ходов ведущих держав в ведении кибервойн, определение их эффективности и результативности. Рассматриваются особенности концептуальных основ войн такого типа, тактики и стратегии, которых придерживаются страны для достижения своих целей, особое внимание уделяется таким странам как США, Россия, Китай.

Предыдущие исследования по данной теме носят фрагментарный, сюжетный характер и не позволяют сформировать целостную картину процессов в мировом киберпространстве. Особенностью данной работы является построение последовательности всех событий и их последствий для изучения общих глобальных процессов и тенденций.

Кибервойны в современном мире приобретают всю более значимую роль. Задачами кибернетического командования всех стран являются подготовка и осуществление полного спектра военных операций в киберпространстве, защита собственных компьютерных сетей, а также препятствие аналогичным действиям противника.[1] Однако их реализация может значительно различаться в каждой конкретной стране.

США, хотя и позиционирует себя как страна без стратегии в ведении кибервойны, все же определила для себя ряд целей, среди которых: готовность для защиты своей страны от разрушительных кибератак, разработка планов кибероперациий для получения преимущества в конфликтах по всему миру, а также поддерживание межнациональных союзов по поддержанию безопасности в киберпространстве.[4]

Китай, в свою очередь, ставит своей целью масштабное переформатирование армии регионального и оборонительного типа в армию, способную вести весь спектр боевых операций.[6] Создание принципиально новых войск является важным стратегическим шагом по формированию современной военной структуры с учетом китайской специфики. [7]

Руководство Российской Федерации понимает всю остроту и серьезность наступающих угроз нового времени. В целях обеспечения безопасности был поставлен ряд задач по разработке конкретных методов по нейтрализации кибер атак.[3] Стратегия России сводится к трем основным направлениям: сдерживанию, предотвращению и разрешению военных конфликтов в кибер пространстве. Не исключается также возможность ответа на угрозы в виртуальном пространстве методами, характерными для реальных войн. В процессе формирования стратегии страны в ведении кибервойны было официально объявлено о создании в вооруженных силах России войск информационных операций. [5]

Современные военные конфликты и их последствия порождают политические сдвиги, социальное напряжение, экономические кризисы, и можно только предполагать, какой оборот примут события в будущем. Большинство стран уже сейчас активно формируют собственную киберармию и выстраивают стратегию войны в информационном пространстве. Поведение каждого государства может оказать большое влияние на социальную и политическую обстановку в мире. Поэтому главными задачами стран для обеспечения и поддержания благополучия является не только формирование собственной стратегии боевых действий, но и четкое понимание тактики противника.

Источники и литература

1) Акопов Г.Л. Феномен информационных войн в сети «Интернет» и его воздействие на современную политику / Государственное и муниципальное управление. Ученые записки СКАГС. – 2011. – N 1. – С. 86-102.
2) Почепцов Г.Г. Информационные войны. Новый инструмент политики / Г.Г. Почепцов. — М.: Алгоритм, 2015. — 256 С.
3) Халидов Д.Ш. Информационная война в России: горькие плоды западничества / Научно-аналитический журнал Обозреватель Observer. – 2011. – N 8. – С.14-25.
4) Armstrong E. R. The Politics of Information: Examining the Conflict Between WikiLeaks and the US Government / University of Ottawa. – 2015. – 143 P.
5) Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций // ТАСС, 2014. [Электронный ресурс.]. URL: http://tass.ru/politika/1179830
6) Chinese hacking activity down sharply since mid-2014, researchers say // The Washington Post, 2016. [Электронный ресурс.]. URL: https://www.washingtonpost.com/world/national-security/chinese-hacking-activity-down-sharply-since-mid-2014-researchers-say/2016/06/20/089703e6-36fd-11e6-9ccd-d6005beac8b3_story.html?utm_term=.12ec55a2c18e
7) U.S., China vow not to engage in economic cyberespionage // The Washington Post, 2015. [Электронный ресурс.]. URL: https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html?utm_term=.0024802dbcce