Секция «Международная безопасность: новые вызовы и угрозы»

Кибервойны как одно из средств реализации внешней политики США

Научный руководитель – Рыбалко Ольга Константиновна

Лукъяненко Веста Владимировна

Студент (бакалавр)

Саратовский государственный университет имени Н.Г. Чернышевского, Институт истории и международных отношений, Саратов, Россия

E-mail: schnitzelfrommars@gmail.com

В век информационных технологий политическое противостояние государств выходит в кибернетическое пространство. Именно Америка стала страной, разработавшей новую технологию ведения войны и тактику ее применения. Такой технологией стала Кибернетическая война, то есть, действия одного национального государства с проникновением в компьютеры или сети другого национального государства с целью нанесения ущерба.

Главным органом, координирующим политику США в киберпространстве, является Кибернетическое командование США. Историю его создания можно разделить на три этапа. Первый:Ноябрь 2006 под эгидой ВВС США начало работу первое Кибернетическое управление[2]. Второй:23 июня 2009 года министр обороны США обязывает Стратегическое командование Вооружённых сил США создать Кибернетическое командование.[6] Третий:21 мая 2010 года Кибернетическое командование официально начало функционировать. На данный момент Киберкомандование объединяет в своей структуре отдельные киберкомандования ВВС, морской пехоты и сухопутных войск.

Перейдем к актуальной для РФ теме - кого из участников международных отношений Соединенные Штаты расценивают как потенциальную угрозу?

КНР. В китайскую концепцию ведения кибервойны входит: использование развивающимися странами нетрадиционных способов ведения войны против господствующих в мире государств, а также использование слабостей в преимуществах противника («жезл ассасина»). Еще один фирменный китайский принцип: украсть какую-либо технологию противника, найти в ней слабое место, разработать свою версию программы.[1]

Политика РФ в киберпространстве считается наиболее опасной, так как она очень похожа на стратегию самой Америки. Тем не менее, РФ и США имеют разные взгляды на само понятие и структуру данного термина, из-за чего и возникают разногласия и постоянные угрозы перерастания кибератак в полномасштабные силовые конфликты.[3]

Потенциальную угрозу для США привносят Израиль и Франция, имеющие киберподразделения, и Иран, Австралия, Южная Корея, Индия, которые, по американским разведданым, способны вести кибервойну. Ввиду потенциальной угрозы не только для США, но и для всего мира, невозможно не упомянуть ИГИЛ, запрещённая в России группировка, которая использует киберпространство для пропаганды и вербовки новых членов террористической организации.

Эффективное обеспечение безопасности возможно лишь при сотрудничестве одного государства с другими. США не исключают эту тенденцию и в отношении кибербезопасности. Цели сотрудничества США с международными партнерами: во-первых, сотрудничество необходимо для создания общей системы сбора информации и оповещения. Во-вторых, США стремятся к выработке общих международных норм киберпространства, базирующихся на совместной работе, прозрачности и надежности. [4]

С какими государствами США сотрудничают в сфере обеспечения кибербезопасности? Специализированное Киберподразделение, создало и контролирует посты постоянных кибер-атташе в Лондоне, Канберре, Оттаве и др. Кибер-атташе, способствуют обмену информации по поводу киберпреступности, а также обеспечивает сотрудничество между этими

государствами и США в данной сфере. США имеют подписанные заявления о сотрудничестве в киберпространстве с Эстонией и Японией.[1] Несмотря на недопонимание между Россией и США, все же присутствует доля сотрудничества в Киберпространстве. Например, «горячая линия» между Москвой и Вашингтоном, а также с 2011 года проходит выработка проекта для Конвенции по ведению кибервойны.[3]

Из чего состоит кибербезопасность США? Изначально США полагали, что цель использования киберпространства заключалась лишь в отстаивании национальных интересов американского государства. Но Соединенные Штаты начали задумываться, «Игра идет не по их правилам», когда поняли, что они - не единственные обладатели кибероружия. Возрастала все большая необходимость в выработке стратегии кибероборонны, а не только наступательной деятельности. Так появился основной документ, регулирующий деятельность США в киберпространстве, - Национальная стратегия по безопасности киберпространства 2003 года. Основные цели Стратегии можно определить как: предупреждение и предотвращение кибератак посредством сокращения уязвимостей в системе кибероборонны, если же атаки произошли - минимизировать последствия. Стратегия по безопасности формулирует пять национальных приоритетов: Национальная система реагирования на инциденты безопасности киберпространства; Национальная программа уменьшения уязвимостей и угроз безопасности; Национальная программа обучения и повышения осознания безопасности киберпространства; Обеспечение безопасности государственного киберпространства; Национальная безопасность и международное сотрудничество по обеспечению безопасности киберпространства.[5]

Подводя итог всему вышесказанному, перечислю некоторые рекомендации, касающиеся политики, осуществляемой Россией в киберпространстве. Невозможно полностью предотвратить угрозы кибератак посредством поиска уязвимостей, поэтому необходимо в первую очередь обеспечить эффективную кибербезопасность. Для этого можно позаимствовать некоторые идеи у американских коллег, например, сотрудничество государственного и частного секторов. Также необходимо вводить такой феномен, как «киберграмотность», чтобы как можно больше людей были знакомы с терминами «киберпространство» и «кибербезопасность». Что же касается отношений РФ и США в отношении киберпространства, то есть сферы в которых сотрудничество потенциально возможно, например, в осуществлении поиска транснациональных киберпреступников, в сфере борьбы с терроризмом, а также совместная работа по созданию специальных принципов недопущения кибератак на критическую инфраструктуру государств.

Источники и литература

1) Кларк Ричард. Третья мировая война: какой она будет? Высокие технологии на службе милитаризма/Е. Карманова .— М.: Изд-во Питер,2011.— 336 с.

2) Шейн Харрис. Кибервойн@: Пятый театр военных действий/А.Никольский — М.: Альпина нон-фикшн, 2016.— 392 с.

3) Козловский Андрей. Сотрудничество России и США в киберпространстве: http://inosmi.ru/military

4) Стратегия Министерства Обороны Соединенных Штатов Америки в сфере киберпространства июль 2011 года: http://constitutions.ru

5) The National Strategy to Secure Cyberspace Feburary 2003: https://www.us-cert.gov

6) US needs 'digital warfare force'. BBC News: http://news.bbc.co.uk