Секция «Мировая политика»

Кибероборона России и США: сравнительный анализ концепций (начало 21 века)

Карасёв Павел Александрович
Аспирант
Московский государственный университет имени М.В. Ломоносова, Факультет мировой политики, Москва, Россия
E-mail: karpaul1@gmail.com

Развитый мир находится под мощным влиянием информационно-коммуникационных технологий (ИКТ). От уровня развития национальной информационной инфраструктуры зависит экономический, оборонный и политический потенциал. Возрастающая зависимость от ИКТ провоцирует появление уязвимости к различным негативным воздействиям, исходящим из информационного пространства.

Международным сообществом признаётся существование угроз: киберпреступности, кибертерроризма, использования информационного пространства в военно-политических целях.[6] В военно-политических целях ИКТ находят применение в существующих и перспективных видах вооружений – создаётся так называемое «умное оружие»; ИКТ используются для ведения разведки и проведения оборонительных и наступательных операций в киберпространстве.

Анализ документов показывает, что с середины 90-х до 00-х в мире к применению ИКТ в военно-стратегическом аспекте относились в большей степени как вспомогательному инструменту – в рамках концепции сетецентричной войны.[5] После 00-х ситуация начала меняться. В США киберпространство признали ещё одним театром военных действий – наряду с воздушным, космическим, водным пространством и сушей. Было сказано, что все разработки и деятельность в киберпространстве носят преимущественно оборонительный характер.[7]

В конце 00-х произошло качественное изменение ситуации. Первым сигналом, что кибероружие становится серьёзным инструментом в руках военных, стало создание в 2010 году в США Киберкомандования – специальной структуры, основными задачами которой являются проведение операций в киберпространстве, и координация взаимодействия по кибероборонe между всеми родами войск.

Союзники США по НАТО уже внесли в свои концепции кибербезопасности положения, в соответствии с которыми позволяется разрабатывать кибероружие.[8] На саммите НАТО в Лиссабоне кибербезопасность включили в число приоритетных направлений.[9] Эксперты НАТО заявляют: «Крупномасштабная атака на командные и контрольные системы альянса или на энергетические сети может привести к ответным оборонным мерам в соответствии с 5 статьей».[1]

Кибероружие существует. Ярким примером является вирус STUXNET, который в 2010 году поразил предприятия ядерной программы Ирана. Кибероперации осуществлялись и раньше, но в этом конкретном случае виртуальная среда впервые повлияла на физический мир. До сих пор идут споры, кто автор этой вредоносной программы, но её сложность свидетельствует о том, что разработку осуществлял подготовленный коллектив. А то, что вирус был нацелен на предприятия ядерного цикла, говорит о наличии политического интереса.

В этой обстановке Россия стремится остановить или как-то регламентировать гонку вооружений в киберпространстве. В 2011 году была представлена Концепция Конвенции об обеспечении международной информационной безопасности.[2] Её целью является распространение общепризнанных принципов и норм международного права на информационную сферу, включая противодействие использованию ИКТ для нарушения международного мира и безопасности, установление мер, способствующих общему социальному и экономическому развитию, невмешательству во внутренние дела других государств, уважению прав и основных свобод человека. Позиция России раскрывается и в документе Министерства обороны России «Концептуальные взгляды на деятельность вооруженных сил Российской Федерации в информационном пространстве»[3], где заложена идея сдерживания, предотвращения и разрешения конфликтов, возникающих в информационном пространстве, а также формирования системы международной информационной безопасности в интересах всего мирового сообщества. Ввиду трудности принятия международным сообществом подобных правил поведения в информационном пространстве, Россия вынуждена развивать собственное кибероружие. О том, что такая работа проводится, косвенно может свидетельствовать проводимый Министерством обороны конкурс, одна из тем которого звучит как «Методы и средства обхода антивирусных систем, средств сетевой защиты, средств защиты ОС»[4], что, очевидно, подразумевает воздействие на информационные системы вероятного противника.

Выводы:

1. В начале 21 века изменилось отношение к использованию ИКТ в военном деле – от концепций сетецентричных войн отделились операции в киберпространстве. Они, в свою очередь, прошли путь от оборонительных к наступательным. Появились киберкомандования. Виртуальный мир стал воздействовать на физический;

2. Большое количество государств уже ведут разработку кибероружия. Позиция России и ряда других государств заключается в необходимости ограничения, а в перспективе – запрета на разработку и применения кибероружия, как инструмента, подрывающего международную стабильность.

Литература

1. NATO warns of strike against cyber attackers /Michael Smith and Peter Warren // The Sunday Times June 6, 2010

2. Конвенция об обеспечении международной информационной безопасности (концепция) // Совет Безопасности РФ. [Официальный сайт]. URL: http://www.scrf.gov.ru/docu (дата обращения: 28.02.2013)

3. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве // Министерство обороны России. [Официальный сайт]. URL: http://ens.mil.ru/files/morf/Strategy.doc (дата обращения: 28.02.2013)

4. Темы научно-исследовательских работ Всероссийского конкурса научно-исследовательских работ среди граждан Российской Федерации в интересах Вооруженных Сил Российской Федерации // Министерство обороны России. [Официальный сайт]. URL:

http://ens.mil.ru/education/contests/more.htm?id=1720@morfSimpleEvent (дата обращения: 28.02.2013)

5. «Концепция развития ВС США до 2010 года» (Joint Vision 2010) [принята в 2006 году] // The Defense Technical Information Center. [Official site]. URL: http://www.dtic.mil/jv (дата обращения: 28.02.2013)

6. Резолюция ГА ООН 54/49 Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности [принята 23.12.1999] // ООН. [Официальный сайт]. URL: http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/RES/54/ (дата обращения: 28.02.2013)

7. «Четырёхлетний прогноз Министерства обороны 2001 года» (Quadrennial Defense Review) [принята 09.2001] // Department of Defense. [Official site]. URL:http://http://www.de (дата обращения: 28.02.2013)

8. The French White Paper on Defence and National Security // Military Education Research Li-brary Network [Official site] URL:http://merln.ndu.edu/whitepapers/france_englis – 48 с. (дата обращения: 28.02.2013)

9. NATO new Strategic Concept // NATO [Official site]. URL:http://www.nato.int/lisbon2010/str concept-2010-eng.pdf (дата обращения: 28.02.2013)