Секция «Мировая политика»

Кибербезопасность и информационная уязвимость ведущих акторов международных отношений

Подолянюк Владислав Юрьевич
Студент
ДонНУ, Исторический факультет, Авдеевка, Украина
E-mail: vlad.podolyanyuk.1993@gmail.com

XXI век характеризуется технологической революцией в сфере коммуникаций и широким использованием компьютерных технологий в деятельности международных организаций и ведущих стран мира. Предпосылкой к возникновению таких понятий как «кибербезопасность» и «киберзащита» является увеличение случаев нелегального вмешательства в персональные системы, а также перехват информации со стороны криминальных структур и террористических организаций. Примером этому могут быть как кибератаки правительственных веб-сайтов Грузии перед началом Российско-Грузинского конфликта 2008 года, так и блокировка почты НАТО от внешних посетителей и временное закрытие доступа на сайт Альянса во время Косовского конфликта. Яркими примерами уязвимости государств могут также послужить «кибератаки» на эстонские частные и государственные институты в 2007 г. и распространение вируса «Стакснет» среди компьютеров иранской АЭС в Бушере в 2010 г., который инфицировал вирусом информационную систему предприятия. Всё это позволяет международному сообществу говорить о появлении «кибервойн» в информационном пространстве.

Целью моего доклада является выявление потенциальных действий в сфере информационной безопасности, а также исследование причин актуализации кибератак и уязвимости ведущих стран мира противостоять этим угрозам. Концептуальной базой моего исследования являются теории «кибернетической войны» и «сетевой войны», выдвинутые сотрудниками RAND Corporation Джоном Арквиллой и Дэвидом Ронфельдтом. В частности, концепция «кибернетической войны» подразумевает, что в ходе будущих военных конфликтов решающую роль будет играть именно информация.

Нормативно-правовой базой исследования проблемы кибербезопасности могут послужить многочисленные документы и резолюции, в том числе:

- конвенция Совета Европы о киберпреступности от 23.11.2001 г.;
- резолюция Генеральной Ассамблеи ООН о создании глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур от 17 марта 2010 г.;
- статья 19 Стратегической концепции обороны и обеспечения безопасности членов Североатлантического договора от 19.11.2010 г. гласит о «координации национальных возможностей по киберзащите»;
- статья 40 Декларации лиссабонского саммита от 20.11.2010 г. провозглашает «о развитии возможности НАТО по реагированию на компьютерные инциденты».

Согласно концепции Джозефа Ная-младшего, выделяют 4 основные категории кибернетических угроз: 1) кибервойна; 2) экономический шпионаж, оба ассоциирующиеся с государством; 3) киберпреступность; 4) кибертерроризм, в большинстве случаев относящиеся к негосударственным акторам МО [3].

Также автор книги «Будущее власти» Джозеф Най утверждает, что в современном мире получит развитие тенденция распространения власти от правительства. Так как современный информационный век, который иногда называют «третьей индустриальной революцией» [5], основывается на быстрых технологических достижениях в области компьютеров и коммуникаций, следовательно, для распространения власти ведущие державы мира, такие как США, Россия, Китай, Великобритания и Франция будут использовать в большинстве случаев современные киберсистемы и киберпространство.

Информационная уязвимость ведущих держав уже проявила себя на многих уровнях. Достаточно примеров, когда в 1998 году Америка пожаловалась на российское правительство по поводу кражи секретов Пентагона и НАСА, что так и не было доказано [4]. Или же пример, когда китайское правительство в 2007 году обвинили в спонсировании кибератак на правительственные компьютеры Германии и частные информационные системы США. Но загвоздка заключается в том, что в современном информационном пространстве:

А) сложно определить круг лиц, привлекаемых к юридической ответственности за совершение киберпреступления;

Б) практически невозможно зафиксировать допустимость и достоверность доказательств по поводу совершения киберпреступления [1].

Уже появление таких понятий как Malware (вредоносное программное обеспечение), DDoS-атаки (нападения типа распространенного отказа в услугах), троянские черви, «Стакснет», фишинг (ограбление частных банковских счетов), кибersквоттинг (регистрация домённых имён с целью их дальнейшей перепродажи) и вообще вся так называемая «the dark side of the internet» свидетельствует об эскалации напряжённости кибербезопасности.

Также отдельное внимание следует уделить так называемой «войне за умы» [2]. Это принципиально иной вид войн в киберпространстве, ведение пропаганды и дезинформация в «человеческом» сегменте сети Интернет. Таким способом, как террористические организации, так и государственные структуры имеют возможность манипулировать сознанием общества. Несмотря на то, что их сложно отнести к холодным войнам в сети Интернет, массовость и результативность таких кибератак не стоит преуменьшать.

Дабы противостоять этому, многие государства и организации проводят техническую работу по обеспечению кибербезопасности. Ярким примером тому является создание после событий 2007 года в Эстонии Центра кибербезопасности НАТО. Также НАТО проводились учения по киберзащите – «Cyber coalition - 2011», в которых участвовали не только государства-члены, но и партнёры НАТО.

Подводя итоги, следует подчеркнуть, что кибербезопасность на данном этапе утвердилась как одна из составляющих международной безопасности стран мира и международных организаций и является важным фактором ведения мировой политики. Информационная уязвимость государств сделала их самыми важными объектами кибератак. Поэтому немедленно необходимо принять меры по профессиональному обеспечению кибербезопасности, всесторонней поддержке и сотрудничеству в этой сфере.

Литература

1. Рассолов И. М. Правовые проблемы обеспечения кибербезопасности в России и зарубежных странах // Политика и общество. 2009. 4 (58). С. 21-26.

2. Смирнов А. А., Житнюк П. П. Киберугрозы реальные и выдуманные // Россия в глобальной политике. 2010. 2.

3. Joseph S. Nye Jr. Cyberspace Wars: The opinion pages: The New York Times. – N.Y., 2011: http://www.nytimes.com/2011/02/28/opinion/28iht-ednye28.html?_r=4.

4. Джозеф С. Най-младший. Информационная уязвимость: Project Syndicate / пер. Н. Жданович. 2008: http://www.project-syndicate.org/commentary/nye65/Russian.

5. Джозеф С. Най-младший. Реальность виртуальной власти: Project Syndicate / пер. Н. Жданович. – 2011: http://www.project-syndicate.org/commentary/nye91/Russian.

Слова благодарности

Особая благодарность выражается старшему преподавателю Донецкого Национального Университета, кандидату исторических наук Каракуцу А. Н. за всестороннюю поддержку в подготовке к конференции.