

Анархия, порядок и агрессия в киберпространстве: военно-политическое измерение

Научный руководитель – Конышев Валерий Николаевич

Скворцова Екатерина Михайловна

Аспирант

Санкт-Петербургский государственный университет, Факультет международных отношений, Санкт-Петербург, Россия

E-mail: palermo.katerina@yandex.ru

Защита киберпространства является одной из наиболее обсуждаемых тем в области безопасности. Преследуя цель достижения стабильности и процветания общества, государства реализует политику по построению информационного общества. Однако наряду с возможностями для развития научно-технический прогресс несет в себе возможности и для дестабилизации.

Наибольшую активность в развитии международной информационной безопасности проявляют США и Россия, однако двустороннее сотрудничество развивается слабо, и государства больше ориентированы на совместную работу с союзниками [3]. Так же предпринимаются усилия по достижению согласия по вопросам кибербезопасности на международном уровне.

Одним из наиболее опасных трендов развития киберпространства является милитаризация Интернета. Эксперты Центра киберзащиты НАТО уверены в том, что информационное пространство может стать «параллельным полем битвы» в будущих конфликтах и полагают, что проведения кибератаки в чистом виде маловероятно и скорее всего, будет сопровождать военные действия в реальном мире. Российская сторона также полагает, что агрессия в киберпространстве будет использоваться с целью усиления эффекта традиционных операций с применением обычных наступательных вооружений [2].

Реакцией на быстрое развитие технологий и появлением в связи с их применением новых угроз безопасности стало создание НАТО за короткий срок системы специализированных механизмов оперативного и стратегического значения. В отсутствие согласованного правового регулирования и общего понимания угроз кибербезопасности на международном уровне подобные механизмы представляют собой угрозу появления центра силы, который будет вырабатывать свое видение информационной безопасности и действовать в одностороннем порядке в соответствии с ним. В условиях таких системных проблем архитектуры киберпространства как трудность идентификации пользователя, определения юрисдикции и использования децентрализованных систем странам, не входящим в блок НАТО, будет трудно защитить граждан своей страны. Односторонняя трактовка «правил игры» в киберпространстве сопровождается решительными и агрессивными действиями в реальном мире, что проявляется в том же задержании российских граждан на территории других стран, без уведомления России. Угрозы, исходящие из виртуального пространства, не дают четкого представления о том, кто является нарушителем информационного суверенитета страны, а значит, стирается грань между киберпреступностью и информационной агрессией со стороны другого государства.

На протяжении многих лет в НАТО обсуждались перспективы и целесообразность применения статьи 5 Североатлантического договора о коллективной обороне в отношении противостояния киберугрозам [4]. В 2010 году НАТО пришло к заключению, что кибератака должна приравниваться к вооруженному нападению, что оправдывает ответный удар военными средствами. Сложность определения настоящего заказчика кибератаки не

позволяла НАТО однозначно подвести данные действия под положения 5 статьи в ходе Лиссабонского саммита 2010 г. и Чикагского саммита 2012 г [7]. Украинский кризис, вызвавший неудовлетворение стран Восточной Европы существующими гарантиями безопасности, в том числе в области кибербезопасности, подтолкнул НАТО к более решительным действиям. В ходе Уэльского саммита 2014 г. было подтверждена возможность ответа Альянса на кибератаку военными средствами. При этом была сделана оговорка, что масштаб подобного ответа будет зависеть от степени воздействия кибератаки и оценки соответствия ее масштаба уровню военного нападения [6].

Непрозрачность принципов принятия решения в области противодействия угрозам в киберпространстве свидетельствует об отсутствии целостного понимания киберугроз и дает широкие возможности для интерпретации каждой отдельной ситуации в соответствии с интересами блока. В НАТО сложившаяся ситуация объясняется тактикой «неопределенности», в условиях которой потенциальный агрессор не будет знать о масштабе кибератаки, за которым будет следовать ответ НАТО. При этом, не раскрывается, что имеется в виду под этим ответом: применение обычных вооружений или совместные усилия по киберзащите членов организации в киберпространстве.

Выработанный подход НАТО является попыткой сдерживания противника в киберпространстве. В то же время перенос противостояния в киберпространство ставит под угрозу существующие механизмы сдерживания оружия. Обезличивание противника и дезориентация в киберпространстве делают противостояние государств более агрессивным. Агрессивность виртуальной среды оказывает серьезное влияние на поведенческие установки людей в реальном мире. В случае применения военных действий в ответ на кибератаку становится маловероятным применение принципа соразмерности ответных действий при обеспечении кибербезопасности [5].

Могло ли открытое информационное пространство стать объединяющим началом - вопрос дискуссионный, но сегодня на лицо то, что киберпространство стало зоной разделения и конфронтации между НАТО и Россией. Анархическая природа интернет - пространства вносит дисбаланс в реальную жизнь, и уже сложно говорить, достаточно ли достигнуто на международном уровне общего понимания по вопросу правового урегулирования отношений в киберпространстве или же проблему можно решить только путем перекройки киберпространства с помощью программного кода. Научно-технический прогресс создал возможность для борьбы за господство в новом пространстве с целью получения новых «трофеев». Если раньше главной ценностью были экономические ресурсы, то сейчас ей является информация. Вопрос в том, успеет ли международное сообщество согласовать «правила действий» военного характера в киберпространстве, можно ли избежать в ответ на кибератаку применения военных действий в реальном мире и какое влияние оказывает необходимость обеспечения кибербезопасности на военную стратегию и тактику государств [1]?

Источники и литература

- 1) Демидов О. Киберкомандование США: уроки для России // Индекс безопасности, №3 (106), Том 19, 2013, стр. 119-123
- 2) Казаковцев А.В., НАТО и кибербезопасность // Вестник Волгоградского государственного университета. Серия 4: История. Регионоведение. Международные отношения. №2, 2012, стр. 109-114
- 3) Карасев П.А., Стратегия информационной безопасности США в XXI веке // Вестник Московского университета, серия 12. Политические науки, №2, Информационная политика, 2013, стр. 89-102

- 4) Ревский А., Кибербезопасность новый подход для коллективной киберобороны//Европейская кибербезопасность: события, оценки, прогнозы, №35, 2014, стр. 12-15
- 5) Jeffrey L. Caton, Distinguishing acts of war in cyberspace: assessment criteria, policy considerations and response implications//Strategic Studies Institute and U.S. Army War College Press, 2014, p.1-102
- 6) Wiesław Goździewicz, Mateusz Krupczyński, Joanna Kulesza, Miron Lakomy, Michał Matyasik, Kate Miller, Tomasz Romanowski, Ryszard Szpyra, Magdalena Szwiec, Joanna Świątkowska, NATO Road to Cybersecurity, The Kosciuszko Institute, 2016, p. 5-77
- 7) Jarno Limnéll, The reality of cyberwar – current concepts and future trends// The European Cybersecurity Journal, 2015, p.39-45