Геополитика

УДК [004.896+327.8](98)(045)

Кибертерроризм как угроза государственной безопасности в Арктическом регионе

© ***Бидная*** Ксения Васильевна, студентка 3-го курса отделения регионоведения и международных отношений института управления и регионологии САФУ имени М. В. Ломоносова. E-mail: kseniya.bidnaya@gmail.com.

Статья представляет собой первый опыт в исследовании возможностей и вероятностей проведения кибернетических атак в Арктическом регионе, а именно: поражение и вывод из строя систем ПРО, а также компьютерных систем управления буровыми вышками, что может принести вред как национальной безопасности государств, так и экологическому состоянию Арктики. Помимо этого в статье освещается вопрос возможного влияния актов кибертерроризма на освоение арктического сектора России, то есть изучаются международные отношения России в «новых политических пространствах» – приполярной зоне и глобальной информационной сфере.

Ключевые слова: *Арктика, кибертерроризм, Россия, США, НАТО.*

Cyber-terrorism as a threat to national security in the Arctic region

© ***Bidnaya*** Kseniya Vasilievna, 3rd year student of the Department of Regional Studies and International Relations of the Institute of Management and Regional Studies NArFU named after M. V. Lomonosov. E-mail: kseniya.bidnaya@gmail.com.

Abstract

This article represents the first experience in the research of possibilities and probabilities of cyber attacks in the Arctic region, namely the defeat and withdrawal from the ABM system, and computer control systems of drilling rigs, which can harm both national security and ecological state of the Arctic. Additionally, this article highlights the question of the possible impact of acts of cyberterrorism on the development of the Arctic sector of Russia, in other words, there are studied International Relations of Russia in the 'new political areas' – circumpilar area and global informative sphere.

Keywords: *Arctic, cyber-terrorism, Russia, USA, NATO.*

Немногим было суждено предугадать, как решительные перемены в обществе изменят соотношение военного противостояния в мире и даже саму природу ведения войны. Настоящее потрясение значит больше, чем просто появление новых машин. Оно обещает реструктуризацию всех человеческих взаимоотношений и ролей.

Э. Тоффлер. «Шок будущего»

Технический прогресс и развитие общества в конце XX века открыли миру немыслимые до этого перспективы и возможности, которые к началу XXI века обусловили вступление современной цивилизации в абсолютно новую эпоху, охарактеризованную американским социологом и футурологом Элвином Тоффлером как информационное общество. Такие коренные изменения, безусловно, влекут за собой новые сложности, социальные конфликты и глобальные проблемы, столкнуться с которыми человечеству придется в XXI веке.

Повсеместная компьютеризация общества выводит информацию на новый уровень, когда она становится коренным элементом войн будущего и кибертерроризма – новой международной угрозы. Использование компьютерных технологий международными организациями, в управлении государственным аппаратом и другими элементами современной инфраструктуры, а также переход на методы компьютерного управления [1] привели к появлению стратегически важных киберобъектов, на которые может быть совершено нападение с террористическими целями, что является главной причиной все большего распространения и возрастания угрозы кибертерроризма в мире.

Помимо этого, коренными проблемными вопросами темы являются: затруднение процесса идентификации источника нападения и определения его местоположения, доказательство совершения киберпреступления и предъявления улик обвиняемому, определение юридической ответственности за совершение преступления в киберпространстве. Перечисленные причины связаны со спецификой киберпространства, с отсутствием нормативно-правовой базы, регламентирующей отношения в киберпространстве, и законодательной классификации противоправных актов в киберпространстве.

Проблема появления терроризма в киберпространстве достаточно нова. Исходя из этого, в научной и практико-управленческой среде еще не сформирован подход к ее изучению и теоритической структуризации. Однако увеличение числа атак на информацию в киберпространстве, а также попытки вывода из строя и нанесения ущерба информационной инфраструктуре, заметно участившиеся в последние годы, говорят о превращении киберпространства в одну из сфер стратегического интереса стран [2], чья особая важность заключается в отсутствии в ней какой-либо нормативно-правовой, а также физической защиты.

В свою очередь рост конфликтного потенциала между Россией и другими государствами в Арктическом регионе обуславливает возможность применения кибернетического оружия с целью вывода из строя элементов информационной инфраструктуры, похищения и перехвата данных, в том числе и стратегически важного назначения.

Военно-стратегическое значение Арктического региона заключатся в его возможной пригодности для проведения большого количества военных операций и маневров в результате изменения климата [3]. Стратегический потенциал Арктического региона признается военными и политическими кругами в США, России и других странах мира.

В «Основах государственной политики Российской Федерации в Арктике на период до 2020 года и дальнейшую перспективу» заявлено о необходимости создания группировок войск (сил) общего назначения, а также поддержания необходимого боевого потенциала группировок войск [4]. Наряду с этим США в президентской директиве по национальной

безопасности (NSPD-66/HSPD-25), посвященной освоению Арктики, говорят о сохранении глобальной мобильности американских военных и гражданских судов и летательных аппаратов во всем Арктическом регионе [5], что представляет опасность для российского сектора Арктики. Помимо этого, «Североатлантический альянс обозначил Арктику зоной своих интересов» [6].

Безусловно, особое стратегическое значение региона влечет за собой возможность его милитаризации. В этом плане РФ большое значение уделяет именно невоенному освоению Арктики, а также ее защите от военной активности [7]. Однако мнения США и НАТО по этому вопросу с Россией несколько расходятся. По заявлению экс-представителя России в НАТО Дмитрия Рогозина, «с учетом изменений климата, изменений условий в Арктической зоне многие натовцы уже сейчас предсказывают, что Северный морской путь станет круглогодичным. Откроются эти льды, они растают, а значит, НАТО точно появится в Арктике. Они давно это планируют. А может быть, там появится при каких-то очень дурных условиях и американская ПРО – на палубе как раз тех самых кораблей» [8].

Технические характеристики систем противоракетной обороны подразумевают их полное управление посредством компьютерных технологий, поэтому именно системы ПРО являются значимым объектом для кибератаки. Стоит сказать, что сегодня существует вероятность взлома и нарушения работы данных систем кибертеррористами [9]. Если же это произойдет, то страна, на которую будет произведена атака, останется беззащитной по отношению к силам противника, санкционировавшего данную атаку. Поэтому можно сказать, что в будущем борьба за Арктику между Россией и США перейдет в плоскость киберпространства.

Помимо этого важно отметить, что другим объектом проведения кибератак в Арктике может быть управление современной буровой установкой, которое также осуществляется посредством компьютерных технологий. Внедрение в электронную систему управления установкой может привести к выводу ее оборудования из строя, к значительному экономическому ущербу стране, а также привести к разливу добываемого сырья и нарушению экологической ситуации в регионе.

Можно предположить, что происшествие такого типа может быть использовано некоторыми странами против России. Основным аргументом США против освоения и разработки Арктики Россией является ее неэкологичность [10]. США путем внедрения жестких экологических стандартов пытаются сосредоточить часть политических полномочий по контролю за разработкой ресурсов Арктики в своих руках [11]. Таким образом, взлом и вывод из строя буровых установок России на шельфе Арктики и последующий разлив нефтепродуктов и загрязнение акватории могут быть использованы как сфальсифицированный аргумент США в подтверждение захватнического и потребительского отношения России к Арктическому региону.

Исходя из вышесказанного, возникает естественная потребность в нормативно-правовой и физической защите стратегических киберсистем России. Отрадно, что уже сегодня Минобороны РФ приступило к разработке концепции кибербезопасности Вооруженных сил, а также к созданию киберкомандования с целью обеспечения информационной безопасности российской армии [12]. Поэтому для стабильного развития страны в будущем, кото-

рое обеспечило бы ей возможность планомерного освоения Арктики и достойное место в стратегической плоскости киберпространства, необходимо создание сильной кибернетической армии, а также защиты против атак других стран.

Литература

1. Возженникова А. В. Международный терроризм: борьба за геополитическое господство. М.: РАГС, 2005.
2. Международные отношения России в «новых политических пространствах»: Космос. Приполярные зоны. Воздушные и морские пространства. Глобальная информационная сфера / Отв. ред. А. Д. Богатуров. М.: ЛЕНАНД, 2011. 272 с.
3. Palmer B. Global warming would harm the Earth, but some areas might find it beneficial // The Washington post. 2012. January 24: URL: http://www.washingtonpost.com/ national/health-science/global-warming-would-harm-the-earth-but-some-areas-might-find-it-beneficial/2012/01/17/gIQAbXwhLQ_story.html (дата обращения: 4.03.2012).
4. Основы государственной политики Российской Федерации в Арктике на период до 2020 года и дальнейшую перспективу // Российская газета. 2009. 27 марта.
5. National Security Presidential Directive and Homeland Security Presidential Directive. URL: http://www.fas.org/irp/offdocs/nspd/nspd-66.htm.
6. Россия обеспокоена активизацией НАТО в Арктике. URL: http://www.ria.ru/ defense_safety/20110706/397987672.html (дата обращения: 2.03.2012).
7. Арктика: зона мира и сотрудничества / Под ред. А. В. Загорского. Москва: ИМЭМО РАН, 2011. 195 с.
8. Дмитрий Рогозин: американская ПРО может появиться на кораблях НАТО в Арктике. URL: http://news.mail.ru/politics/2931168/print/ (дата обращения: 15.02.2012).
9. Mannes A., Hendler J. The first modern cyber war? // The Guardian. 2008. August 22. P. 7.
10. Юргенс И. Ю. Отношения Россия – США: к новой повестке дня. М.: Экон-Информ, 2009. С. 43.
11. Конышев В. Н., Сергунин А. А. Арктика на перекрестье геополитических интересов // Мировая экономика и международные отношения. 2010. № 9. С. 43–53.
12. Белянинов К. Если завтра кибервойна // Огонек. 2010. № 19. С. 28–27.

Рецензент – Лукин Юрий Фёдорович,
доктор исторических наук, профессор.