Секция «Международная безопасность: традиционные вызовы и угрозы»

Влияние киберпространства на концепцию «воздушной мощи»

Научный руководитель – Веселов Василий Александрович

Котова Ю.А.[1], *Голубев А.В.*[2]

1 - Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Москва, Россия, *E-mail: YuliaKUrusova@gmail.com*; 2 - Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Москва, Россия, *E-mail: artyom_golubev99@mail.ru*

Природа современных конфликтов требует изменений в концепциях «воздушной мощи». В первую очередь это связано с серьезным развитием киберпространства за последние 25 лет. Относительно новым доменом для сложных военных систем является именно эта коммуникационная сфера, среди главных особенностей которой выделяют возможность пронизывать всю окружающую среду (людей и техносферу) и, в случае необходимости, парализовывать ее движение или функционирование. Большинство современных военных систем настолько тесно переплетены с киберпространством, что зависят от него в своих основных операциях. Кроме того, многие из них прямо или косвенно связаны с другими военными системами.

В процессе изучения темы было установлено, что на первый план выходят новые информационные технологии, внедрение которых в военную сферу направлено на усиление боевых возможностей войск, но уже не только за счет повышения огневых, маневренных и прочих характеристик индивидуальных платформ, но и в первую очередь за счет сокращения цикла боевого управления в операции. Сама область киберпространства может использоваться различными способами. Среди основных киберугроз все чаще выделяют такие как сбор сведений об этих системах для кражи технологий и ускорения собственных возможностей; использование их для разработки контрмер или в качестве средства прямой атаки на военные системы других стран. Вместе они являются критически важными для достижения военно-политических целей.

В качестве жизненно важного компонента проецирования силы, в том числе воздушной сферы, киберпространство превзошло свою оценку в качестве инструмента, который теперь признан не только особо важным для обеспечения выполнения поставленных задач, но и сам по себе областью действий. На основе анализа военных конфликтов конца XX - начала XXI века авторы смогли выявить основные тенденции ведения войн нового типа, в которых:

1) главный упор делается на высокоточное оружие;
2) используются разведывательно-информационно-управляющие системы.

Война в Персидском заливе 1991 года была первым конфликтом, наглядно продемонстрировавшим значение радиоэлектронной борьбы для ведения современной воздушной войны. К тому же, со времен второй мировой войны ни в одном из вооруженных конфликтов не было такой высокой интенсивности использования авиации как во время проведения операции "Буря в пустыне"[3][5], что лишь подчёркивает определяющую роль воздушного пространства. Как мы видим, кибервозможности позволяют использовать многие дополнительные функции (например, электронную атаку, слияние датчиков и связи), которые дают ВВС преимущество над потенциальными противниками.

Актуальность исследования обусловлена тем, что быстро развивающиеся технологии предполагают пересмотр концепций «воздушной мощи», что в свою очередь отразится на эволюции новых типов военной и гражданской воздушной авиации. Уже сейчас, говоря, например, о концепции «рой», эксперты придерживаются мнения, что разрушение подобного вида оружия завязано исключительно на использовании аналогичного беспилотника или применении кибертехнологий[1][2].

Первое десятилетие XXI века поставило проблему многомерного сдерживания (Cross-Domain Deterrence) на первое место в сообществе оборонной политики США[4]. К сожалению, данная сфера пока недостаточно изучена в отечественной науке. Авторы убеждены, что в ближайшем будущем правительства многих стран все чаще будут сталкиваться с проблемой пересмотра своего отношения к киберпространству.

В связи с этим актуальность выбранной проблемы заключается еще и в том, что киберпространство, являясь сложным, быстро меняющимся и трудно прогнозируемым, регулируется системами, которые лучше подходят для простых, стабильных и предсказуемых сред, что приводит к значительным пробелам в управлении кибербезопасностью. Современное развитие этого пространства и его влияние на другие среды нуждаются в более тщательном изучении.

Источники и литература

1) Веселов В.А., Фененко. А.В. “Воздушная мощь» в мировой политике” // Международные процессы. Том 14. Номер 3 (46). Июль–сентябрь / 2016, стр. 6-27

2) Леонов А.В., Пронин А.Ю. “О роли и месте сетевых архитектур типа «рой» в концепциях современных войн и необходимости их военно-экономической оценки”// Журнал Вооружение и экономика 3(40)/ 2017 г., стр. 3-13, ISSN 2071-0151 URL: http://sc.mil.ru/files/morf/military/archive/ViE-40.pdf дата обращения: 24.02.2019

3) Новиков А., Галин Л. “Подавление системы ПВО Ирака в операции "Буря в пустыне" - Зарубежное военное обозрение №9 1991г, URL: http://pentagonus.ru/publ/100-1-0-193 дата обращения: 24.02.2019

4) Gartzke E., Lindsay J. “Cross-Domain Deterrence: Strategy in an Era of Complexity” - July2014,URL: https://quote.ucsd.edu/deterrence/files/2014/12/EGLindsay_CDDOverview_20140715.pdf дата обращения: 24.02.2019

5) Kopp C. “Operation Desert Storm The Electronic Battle Parts” 1-3, URL: http://www.ausairpower.net/Analysis-ODS-EW.html дата обращения: 24.02.2019

6) Snyder D., Powers J. D., Bodine-Baron E., Fox B., Kendrick L., Powell M.H. “Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles”// RAND® corporation - S.M., CA - 2015, ISBN: 978-0-8330-8900-7 URL: https://www.rand.org/pubs/research_reports/RR1007.html дата обращения: 24.02.2019