УДК 327.83

ДЕЯТЕЛЬНОСТЬ ЧАСТНЫХ ВОЕННЫХ КОМПАНИЙ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В ВЕК ЦИФРОВОЙ ТРАНСФОРМАЦИИ

А.Я. Зайцев

специалист по учебно-методической работе кафедры российской политики факультета политологии

Московского государственного университета им. М.В. Ломоносова

e-mail: zayts214@rambler.ru

Аннотация: В статье рассматривается деятельность частных военных компаний как угроза национальной безопасности государств в условиях цифровизации. Описываются различные риски и угрозы, которые могут возникнуть учетом развития цифровых технологий.

Ключевые слова: частные военные компании, цифровые технологии, национальная безопасность, вызовы и угрозы современности.

THE ACTIVITIES OF PRIVATE MILITARY COMPANIES AS A THREAT TO NATIONAL SECURITY IN THE AGE OF DIGITAL TRANSFORMATION

A.Y. Zaytsev

Abstract: The article examines the activities of private military companies as a threat to the national security of states in the context of digitalization. Various risks and threats that may arise taking into account the development of digital technologies are described.

Keywords: private military companies, digital technologies, national security, challenges and threats of our time.

С развитием и появлением новых технологий, военная сфера стала адаптироваться к происходящей цифровой трансформации, осуществляя внедрение различных разработок в производство военизированной техники, высокоточных систем, практику военного управления и т.д. [1]

В современных конфликтах XXI большую роль стали играть частные военные компании, которые привлекаются государствами для осуществления различного рода задач по всему миру.

Частные военные компании в современном мире представляют собой хорошо организованные коммерческие структуры, которые предоставляют широкий спектр военно-охранных услуг. В условиях большой конкуренции сотрудники таких организаций стремятся осваивать новые виды вооружения, так как спрос на высококвалифицированных специалистов не ограничен. При этом с развитием глобализации некоторые компании все больше превращаются в транснациональные корпорации, предоставляя услуги различным государствам, международным и неправительственным организациям [2].

Следует констатировать, что деятельность частных военных компаний в век цифровых технологий может нести угрозу национальной безопасности государств, так как сотрудники ЧВК все активнее осваивают новейшие технологии и могут с их помощью осуществлять противозаконные действия, нарушающие международное и уголовное право.

Сотрудниками ЧВК для работы могут быть арендованы даже специальные помещения, так как некоторые организации получают узкоспециализированные государственные заказы, связанные с информационной сферой: сотовая связь, радиосигналы, Интернет, социальные сети и т.д.

Большую угрозу представляет риск утечки данных. Государственные структуры или любые другие организации, содержащие информационные данные, могут подвергнуться хакерской атаке [3], осуществляемой частной военной компанией. Информация, полученная таким способом, может стать эффективным инструментом в процессе осуществления давления на противника.

Также необходимо отметить повышение уровня киберугроз. Осуществление кибератак, а также наращивание возможностей внешнего информационно-технического воздействия на инфраструктуру другого государства может стать серьезным вызовом в ситуации, когда существует отставание от ведущих иностранных стран в развитии конкурентоспособных информационных технологий.

Сотрудники ЧВК могут осуществлять киберпреступления [4] будучи частью какой-либо четко выработанной стратегии, осуществляемой государством агрессором наравне с применением экономических, политических, информационно-психологических и военных инструментов давления [5].

Вместе с эти частные военные компании по причине трансграничного характера своей деятельности могут также оказывать услуги по предотвращению и противодействию угрозам, связанным с цифровизацией. Применение различных контрмер в целях обеспечения безопасности государства будет эффективно при наличие превентивной оценки уязвимостей и прогнозирования рисков [6].

В будущем угрозы будут лишь увеличиваться, а методы кибератак станут гораздо более изощренными. В такой ситуации "государства должны научиться адаптироваться к синергетической модели, где государственно-частное партнерство сможет обеспечить удовлетворительный уровень защиты" [7, с. 6], и что обеспечение государственной и корпоративной безопасности сможет гарантировать безопасность всего населения той или иной страны.

Библиографический список

1. Карлова Е.Н. Талынев В.Е. Возможности и ограничения использования цифровых технологий военнослужащими в условиях цифровой трансформации общества // Вестник Московского государственного лингвистического университета. Серия общественные науки. – 2020. – № 2 (839).

2. Манойло А.В. Зайцев А.Я. Международно-правовой статус частных военных компаний // Вестник Российской Академии наук. – 2020. – Т. 90. – № 1.

3. Алекперов И.Д., Горбачев А.А. Типы угроз кибербезопасности и способы борьбы с хакрестом // Интеллектуальные ресурсы – региональному развитию. – 2021. – № 2.

4. Халин В.Г. Чернова Г.В. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски // Управленческое консультирование. – 2018. – № 10.

5. Паламарчук Ю.Е. Кибертерроризм: понятие, проблемы противодействия // Интеллектуальные ресурсы – региональному развитию. – 2021. – № 1.

6. Опасности цифровизации или цифровизация в опасности // РБК [Электронный ресурс]. – Режим доступа: https://spb.plus.rbc.ru/news/5cb448c57a8aa90a3814c68e (дата обращения 21.12.2021)

7. Гаранина И.Г., Кулешова Г.П., Скирда М.В. Международно-правовое регулирование частных военных и охранных предприятий: учебно-методическое пособие / Мар. гос. ун-т. – Йошкар-Ола, 2018.